SENTRY SOFTWARE
www.sentrysoftware.net

Hardware Sentry KM for PATROL®

User Guide

Supporting

Hardware Sentry KM for PATROL

Version 1.5.00

March 2008

BMC SOFTWARE VALIDATED MARKETZONE

Contacting BMC Software

You can access the BMC Software Web site at http://www.bmc.com/. From this Web site, you can obtain information about the company, its products, corporate offices, special events, and career opportunities.

United States and Canada		Outside United States and Canada	
Address	BMC Software, Inc. 2101 CityWest Blvd. Houston TX 77042-2827	**Telephone**	(01) 713 918 8800
		Fax	(01) 713 918 8000
Telephone	713 918 8800 or 800 841 2031		
Fax	713 918 8000		

Copyright 2006 BMC Software, Inc. or licensors, as an unpublished work. All rights reserved.

BMC Software, the BMC Software logos, and all other BMC Software product or service names are registered trademarks or trademarks of BMC Software, Inc.

IBM is a registered trademark of International Business Machines Corporation.

DB2 is a registered trademark of International Business Machines Corporation.

Oracle is a registered trademark, and the Oracle product names are registered trademarks or trademarks of Oracle Corporation.

All other trademarks belong to their respective companies.

BMC Software considers information included in this documentation to be proprietary and confidential. Your use of this information is subject to the terms and conditions of the applicable End User License Agreement for the product and the proprietary and restricted rights notices included in this documentation.

Restricted Rights Legend

U.S. Government Restricted Rights to Computer Software. UNPUBLISHED -- RIGHTS RESERVED UNDER THE COPYRIGHT LAWS OF THE UNITED STATES. Use, duplication, or disclosure of any data and computer software by the U.S. Government is subject to restrictions, as applicable, set forth in FAR Section 52.227-14, DFARS 252.227-7013, DFARS 252.227-7014, DFARS 252.227-7015, and DFARS 252.227-7025, as amended from time to time. Contractor/Manufacturer is BMC Software, Inc., 2101 CityWest Blvd., Houston, TX 77042-2827, USA. Any contract notices should be sent to this address.

Customer Support

You can obtain technical support by using the Support page on the BMC Software Web site or by contacting Customer Support by telephone or e-mail. To expedite your inquiry, please see the section "Before Contacting Sentry Software" given below.

Support Web Site

You can obtain technical support from Sentry Software 24 hours a day, 7 days a week at http://www.bmc.com/support_home. From this Web site, you can

- read overviews about support services and programs that BMC Software offers
- find the most current information about BMC Software products
- search a database for problems similar to yours and possible solutions
- order or download product documentation
- report a problem or ask a question
- subscribe to receive e-mail notices when new product versions are released
- find worldwide BMC Software support center locations and contact information, including e-mail addresses, fax numbers, and telephone numbers

Support by Telephone or E-mail

In the United States and Canada, if you need technical support and do not have access to the Web, call 800 537 1813. Outside the United States and Canada, please contact your local support center for assistance. To find telephone and e-mail contact information for the BMC Software support center that services your location, refer to the Contact Customer Support section of the Support page on the BMC Software Web site at http://www.bmc.com/support_home

Before Contacting BMC Software

Before you contact Sentry Software, please ensure you have the following information available so that Customer Support can begin working on your problem immediately:

Product information

- product name
- product version (release number)
- license number and password (trial or permanent)

Operating system and environment information

- machine type
- operating system type, version, and service pack or other maintenance level such as PUT or PTF
- system hardware configuration
- serial numbers
- related software (database, application, and communication) including type, version, and service pack or maintenance level

Sequence of events leading to the problem

Commands and options that you used

Messages received (and the time and date that you received them)

- product error messages
- messages from the operating system, such as file system full
- messages from related software

Table of Contents

OVERVIEW **6**

GETTING STARTED **8**

HOW DOES IT WORK? 9

INTEGRATING HARDWARE SENTRY 10

THE NEED FOR MANUFACTURER-SPECIFIC HARDWARE MONITORING SOFTWARE 11

USING HARDWARE SENTRY TO MONITOR HARDWARE 12

SUPPORTED PLATFORMS AND REQUIREMENTS 13

INSIDE HARDWARE SENTRY 16

MONITORING **19**

THE BASICS 20

MONITORING TEMPERATURES, FANS, VOLTAGES AND POWER-SUPPLIES 29

MONITORING DISKS 32

MONITORING PROCESSORS, MEMORY MODULES AND NETWORK INTERFACES 34

MONITORING REMOTE SYSTEMS 37

DETECTING MISSING DEVICES 42

MONITORING CONNECTORS 43

THRESHOLDS, ALERTS & NOTIFICATION **44**

THRESHOLD MECHANISM SELECTION 45

MODIFYING ALERT THRESHOLDS ON PARAMETERS 47

TUNE THRESHOLD TOLERANCE 50

ALERT AFTER *N* TIMES – ADVANCED ALERT SETTINGS 51

ALERT ACTIONS 52

EDITING ALERT ACTIONS 53

ALERT ACTION MACRO VARIABLES 58

INTERNAL KM ISSUES NOTIFICATION 61

INTRUSION DETECTION ALERTS 62

NETWORK LINK ALERTS 63

Unknown Status Management 64

Configuration and Administrative Tasks 65

Set connection, credentials and connectors on the local host 66

Customize the discovery cycle 72

Customize the polling interval 73

Enter a license key for Hardware Sentry 74

Distribute the license over several computers 76

Pause the monitoring of an object 77

Reinitialize the KM 78

Restore the monitoring of a device after removal 80

Show an instant Hardware Health report 82

Schedule Hardware Health reports 84

Terminate the monitoring of a device 88

Trigger a KM discovery 89

Display labels in the UNIX Console mode 90

Troubleshooting 91

Enabling the debug mode 92

Hardware Sentry shows nothing 93

Shows/Monitors Network Interfaces, but no other components 94

Servers running Windows or Linux 96

Special note about SNMP on Windows Server 2003, 2008 97

Unable to see Disk Controller 98

Overview

Hardware Sentry KM for PATROL enables administrators to monitor the hardware of their diverse servers. This is a single KM that is able to monitor the hardware of different server brands: IBM®, HP®, DELL®, Sun Microsystems®, NEC®, Fujitsu-Siemens® and many others.

Once installed, Hardware Sentry requires no configuration and automatically detects the environment and starts monitoring the hardware: status of the disks and the RAID controllers, temperature of the system, speed of the fans, power supplies, network interfaces etc.

As the solution connects to vendor-specific instrumentation agents on the servers to collect hardware information, it is vital to install these "agents" on your systems prior to installing the KM.

Important

Please refer to the platform-specific guides for information on details on how to install the vendor-specific instrumentation agents. They are a prerequisite on the managed systems for Hardware Sentry to function.

This document explains how to use BMC® Performance Manager for Hardware.

This guide details all the available features, and explains how the monitoring functions for the different hardware components. The document also gives you a brief look "inside" Hardware Sentry, to help understand how the product works. A troubleshooting section lists the most frequently asked questions.

The product documentation for BMC Performance Manager for Hardware consists of:

1. Installation Guide – for details on how to install and run the product.
2. User Guide – current document
3. Reference Guide – for details on application classes, menu commands, parameters, configuration variables and connector and platform details
4. Release Notes – tells you about the enhancements in this version.
5. Platform-specific Guides – for details on the installation of vendor-specific hardware agents

Installation procedure in a nutshell

Prerequisites

1. Hardware Sentry is a KM for PATROL and therefore needs to be installed on every managed system with an Agent, Consoles, Console servers and PATROL Central Web-edition.
2. Minimum version of PATROL should be 3.4.11.
3. Servers to be monitored should have their respective instrumentation agents installed. See the Platform-specific guides for details.
4. Product packages to be downloaded from BMC EPD or Sentry Software Web site.
5. Latest BMC Software Installation Utility to be downloaded from the BMC FTP site.

Installation

1. Store the installation utility and the product packages in the same folder.
2. Click first on the installation utility and then on the product package file.
3. Follow the installation wizard.
4. For optimal performance, configure PATROL agents to preload the Hardware Sentry KM.
5. Enter license applicable license keys…and you are all set to use BMC Performance Manager for Hardware.

Please refer to the Installation Guide for details.

Getting Started

This section gives you brief glimpse at how Hardware Sentry works and what hardware components it monitors.

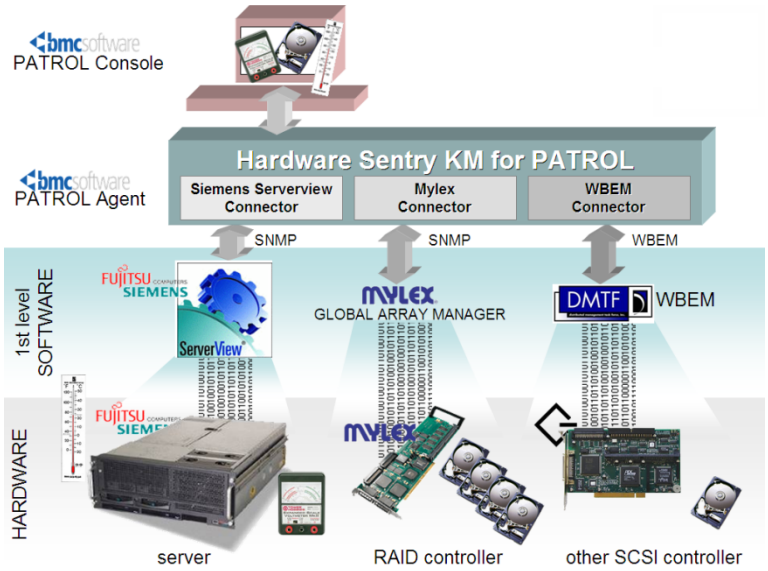
How does it work?

Hardware Sentry is a KM that enables PATROL to monitor computer hardware (disk status, temperatures, CPU, power supplies etc.).

It gathers hardware information from different sources such as manufacturer-specific agents, standard management technologies, SNMP, WBEM, etc., and displays this information within the PATROL framework.

In order to work properly, Hardware Sentry needs certain hardware information sources to be available. Depending on the platform, it relies on manufacturer-specific agents and/or on standard management technology such as WBEM or SNMP. On startup, Hardware Sentry automatically detects which hardware information source is available and then uses this poll data on the hardware health of the computer. Hardware Sentry collects such data from each server and reports in your PATROL console.

The image below represents how Hardware Sentry monitors the hardware of a Fujitsu-Siemens® computer:

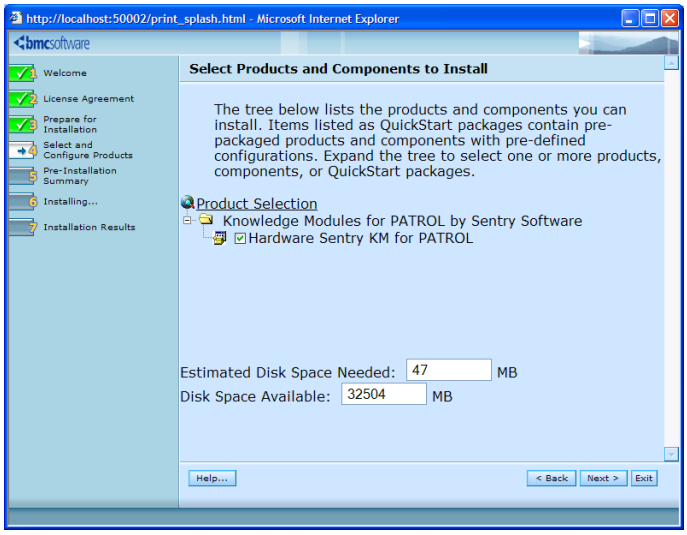


- The Siemens® ServerView® agent shows the temperatures, the fans, the power supplies and the voltages of the Siemens computer through SNMP
- The Mylex® GAM Server shows the status of the physical and logical disks of the Mylex® RAID Controller through SNMP
- The Windows WMI provider shows the status of the physical disks attached to the standard SCSI controller through WBEM
- Hardware Sentry detects and automatically connects to all three information sources (Siemens ServerView, Mylex GAM Server and Windows WMI provider) and gathers only useful hardware information from them and reports it within the PATROL framework

Integrating Hardware Sentry

The Hardware Sentry package is to be installed using the BMC Software Installation Utility. Hardware Sentry is a knowledge module (KM) for BMC Software PATROL. Therefore it must be installed on the following components of the PATROL framework:

- PATROL Agents
- PATROL Consoles
- PATROL Console Server
- PATROL Central – Web Edition


http://localhost:50002/print_splash.html - Microsoft Internet Explorer
bmcsoftware
Welcome
License Agreement
Prepare for Installation
Select and Configure Products
Pre-Installation Summary
Installing...
Installation Results
Select Products and Components to Install
The tree below lists the products and components you can install. Items listed as QuickStart packages contain pre-packaged products and components with pre-defined configurations. Expand the tree to select one or more products, components, or QuickStart packages.
Product Selection
Knowledge Modules for PATROL by Sentry Software
Hardware Sentry KM for PATROL
Estimated Disk Space Needed: 47 MB
Disk Space Available: 32504 MB
Help...
< Back
Next >
Exit

Like any other KM, the active part of Hardware Sentry resides on the PATROL Agent.

A PATROL Agent must be installed on each server whose hardware is to be monitored, and Hardware Sentry must be installed on each PATROL Agent.

Once Hardware Sentry is integrated within the PATROL framework, the hardware information and status of the monitored servers will be available in the PATROL interface.

Please refer to the Installation Guide for details on the installation procedure.

Hardware Sentry is able to monitor certain components of a system remotely through the network using SNMP and WMI protocols since version 1.4.00. However, this does not imply that *all* servers can be monitored remotely. For further details, please see the section: *Monitoring*

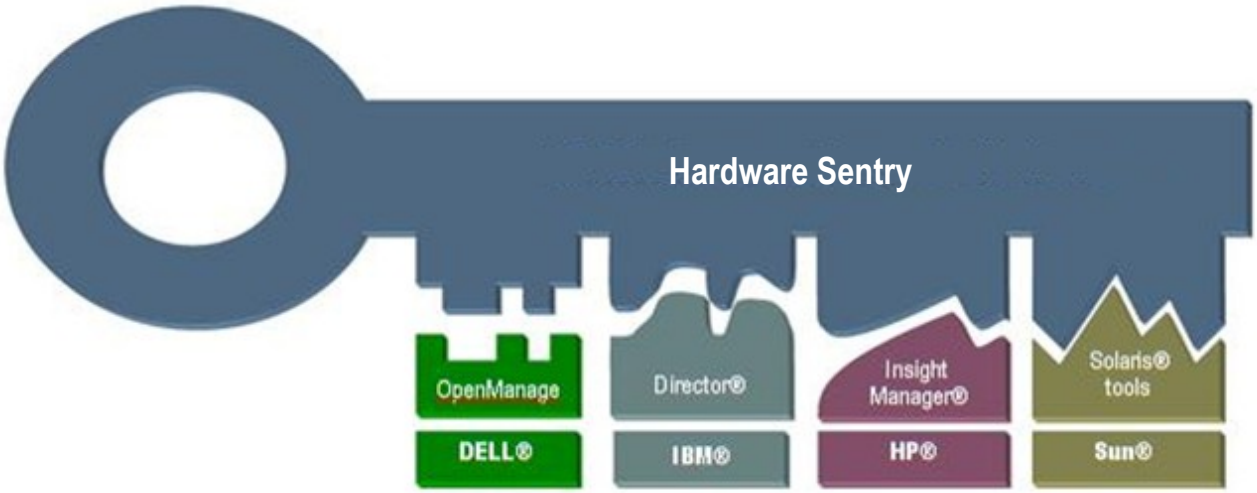
The need for manufacturer-specific hardware monitoring software

Often, the standard operating system layer is not a sufficient hardware information source and most computers require an additional manufacturer-specific agent for Hardware Sentry to function properly. In most cases, server vendors provide the required hardware monitoring agent for their server models.

Depending on the platform, a single agent could monitor the temperatures, fans, voltages, power supplies and RAID systems, or, the platform may require separate agents for environment and disk monitoring.

For example: The IBM Director Agent monitors and provides information about temperatures, fans, voltages, power supplies and the ServeRAID disks for IBM xSeries and Netfinity servers. On the other hand, the Siemens ServerView Agent only monitors the sensors on the motherboard of the server (temperatures, voltages, fans and power supplies) and so the Mylex GAM Server is required to monitor the Mylex RAID controller of the server.

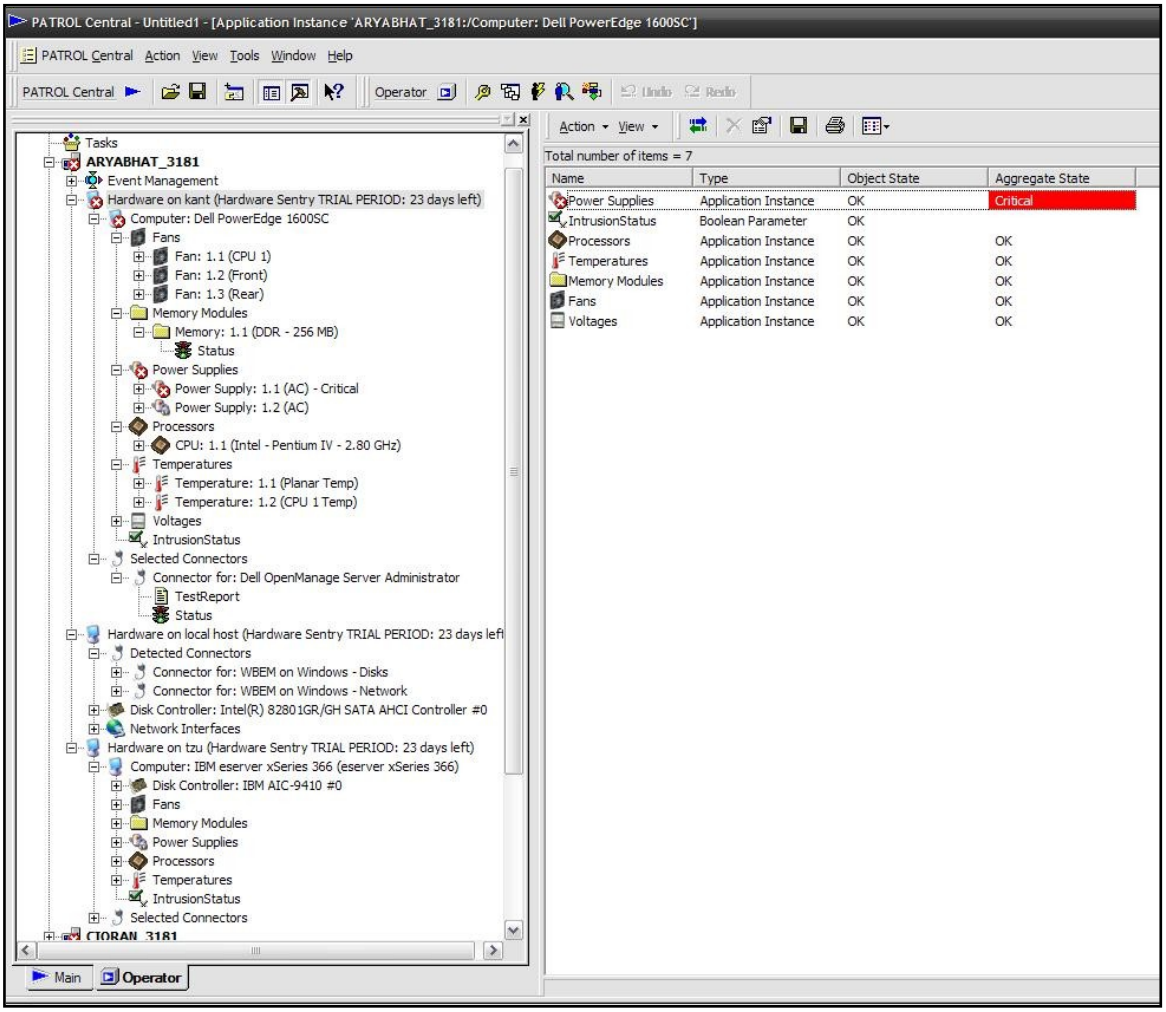
Please refer to the Installation Guide and the Platform-specific guides for further details.



Using Hardware Sentry to monitor hardware

Once Hardware Sentry is installed and integrated into the PATROL framework and the hardware information sources are available, the hardware information of the monitored computers will be displayed in the PATROL Consoles (PATROL® Classic Consoles and PATROL® Central).

The operators and administrators just have to look at the PATROL Consoles to see the hardware health of their monitored servers in exactly the same way they see the operating system or database health. Under each server icon, a tree represents all the monitored hardware for this server.



Supported Platforms and Requirements

The BMC Software PATROL Agent must be installed on each managed system and its version should be at least 3.4.11.

For Hardware Sentry to collect information from a managed system, it requires specific instrumentation agents or system management tools to be present on the managed system.

Typical Platform	Operating System	Required Instrumentation Agent/System Tools
Dell PowerEdge	Microsoft Windows	Dell OpenManage Server Administrator, WMI
Dell PowerEdge	Linux	Dell OpenManage Server Administrator, Linux system commands, SmartMonTools
Fujitsu-Siemens BX Blade servers	N/A	Fujitsu-Siemens Management Blade
Fujitsu-Siemens PRIMERGY	Microsoft Windows	Fujitsu-Siemens Serverview / Fujitsu-Siemens ServerView RAID Agent / Promise FastTrack SNMP Agent / LSI GAM Server / LSI MegaRAID SAS SNMP Agent / LSI MegaRAID PowerConsole / Mylex GAM Server , WMI
Fujitsu-Siemens PRIMERGY	Linux	Fujitsu-Siemens Serverview / Fujitsu-Siemens ServerView RAID Agent / Promise FastTrack SNMP Agent / LSI GAM Server / LSI MegaRAID SAS SNMP Agent / LSI MegaRAID PowerConsole / Mylex GAM Server, Linux system commands, SmartMonTools
HP C-Class BladeSystem	Windows	HP Insight Management Agent
HP C-Class BladeSystem	Linux	HP Insight Management Agent
HP P-Class BladeSystem	N/A	iLO
HP AlphaServer	Tru64	HP Insight Management Agent
HP 9000	HP-UX	HPU system tools
HP Integrity	Windows	HP Insight Management Agent
HP Integrity	Linux	HP Insight Management Agent
HP Integrity	HP-UX	HPUX system commands + MP/GSP

Typical Platform	Operating System	Required Instrumentation Agent/System Tools
HP Proliant	Windows	HP Insight Management Agent, WMI
HP Proliant	Linux	HP Insight Management Agent, Linux system commands, SmartMonTools
HP NetServer	Windows	Toptools
HP SuperDome (Itanium)	Windows	HP Insight Management Agent
HP SuperDome (Itanium)	Linux	HP Insight Management Agent
HP SuperDome (Itanium)	HP-UX	HP-UX system commands + MP/GSP
HP SuperDome (PA-RISC)	HP-UX	HP-UX system commands + MP/GSP
IBM RS/6000, IBM pSeries, IBM eServer p5	IBM AIX	IBM AIX system commands
IBM xSeries, IBM NetFinity	Microsoft Windows	IBM Director Agent ,WMI
IBM xSeries, IBM NetFinity	Linux	IBM Director Agent , Linux system commands, SmartMonTools
NEC Express5800	Microsoft Windows	NEC ESMPRO Agent, WMI
NEC Express5800	Linux	NEC ESMPRO Agent
StorageTek LSeries	Storage	StorageTek LSeries SNMP Agent
StorageTek SreamLine	Storage	StorageTek StreamLine SNMP Agent
Sun Fire (SPARC)	Solaris	Solaris system commands
Sun Fire (SPARC, T1, T2)	Solaris	Solaris system commands + Sun ALOM card (Sun Advanced Lights-Out Management)
Sun Fire F12K, F15K, F20K, F25K	Solaris	Solaris system commands + SMS utilities intsalled on the system controller
Sun Fire X64	Solaris	Ipmitool, lsiutil
Sun Fire X64	Linux	Ipmitool, lsiutil

Important

Generally server manufacturers furnish instrumentation agents and system tools for free and these are either found on the CD-ROM provided with the server or, on the manufacturer's web site. Unless mentioned otherwise, the manufacturer's instrumentation agent must be installed on the monitored server for Hardware Sentry to function properly.

For details on how to install the required instrumentation agent on the systems, please refer to the **platform-specific guides** available on the Hardware Sentry page of the Sentry Software website.

As Sentry Software is continuously working on the support of new hardware information, sources and new platforms that can be monitored with Hardware Sentry will continue to grow.

Please check our web site www.sentrysoftware.net to find the latest updates. Updates are in the form of patches for Hardware Sentry are free and do not need an upgrade of the KM itself, unless there are structural changes.

Hardware components monitored

Depending on the managed system, Hardware Sentry monitors:

- Disks (RAID and non-RAID disks)
- Disk Enclosures
- Fans
- Memory modules
- Network interfaces
- Power supplies
- Processors
- Temperature
- Voltage

Important

For details on what hardware components are detected on each system, please see the Connectors & Platforms Reference Table in the Reference Guide and click on the *Connector Name* applicable to your system/typical platform.

All product documentation is also available in an online format accessible from within the product as well as in the Hardware Sentry Online Technical Library on the Sentry Software website.

Inside Hardware Sentry

Architecture

Hardware Sentry is principally composed of:

- A common hardware monitoring engine (MS_HW_*.km KM classes and ms_hw_*.lib PSL libraries that run with the PATROL Agent of each monitored computer)
- Several connector files (MS_HW_*.hdf) that are platform-specific

Upon startup, Hardware Sentry tests each connector in order to detect which hardware information sources are available (manufacturer-specific hardware agents, standards instrumentation layers, etc.). This is called the "detection process".

Once Hardware Sentry knows which hardware information sources are available and can be connected to, it tries to discover the hardware environment by querying these selected hardware information sources, as described in the corresponding *.hdf files. This is called the "discovery process".

Finally, when the detection and discovery processes are complete, Hardware Sentry starts collecting data about the discovered hardware environment (status, temperatures, voltages, etc.) by querying the detected hardware information sources as described in the corresponding *.hdf files. This is called the "collection process".

The table below shows the synopsis of the actions performed by Hardware Sentry.

Macro	Description	Corresponding PATROL process
Activation	Activates the MS_HW_MAIN class.	PRE-DISCOVERY process of the MS_HW_MAIN class. Executed once on the PATROL Agent startup.
License check	Creates the MS_HW_MAIN icon. Look for a valid license key. Activates all of the Hardware Sentry classes.	DISCOVERY process of the MS_HW_MAIN class. Executed every hour (default period).
Detection Process	Tests each connector in order to detect which hardware information sources are available and can be connected to.	
Discovery Process	Discovers the hardware environment by querying the previously detected hardware information sources. Creates the other class instances (MS_HW_TEMPERATURE, MS_HW_PHYSICALDISK, etc.)	
Collection Process	Polls previously detected hardware information sources to gather data about the hardware environment.	Collector parameters of the MS_HW_MAIN class: fanColl, logicalDiskColl, otherDeviceColl, etc. Executed every 2nd minute (default period).

The Connectors

Each connector is an ".hdf" file that is dedicated to one hardware information source. The purpose of each connector file is to describe how Hardware Sentry should connect to the hardware information source available on a platform and which information is available through this source. For example, MS_HW_Director41NT.hdf will describe how to get information from the IBM Director 4.1 Agent and then monitor an IBM xSeries server.

An ".hdf" file can tell the Hardware Sentry engine to do the following actions:

- Query a SNMP agent (get, get_next, and tables)
- Execute a WBEM query
- Execute an OS command

Each ".hdf" file uses a mix of these possible actions with some computing capabilities to make Hardware Sentry gather useful data in a given hardware information source.

Note on HDF files

The ".hdf" files are located under the "`MS_HW_hdf`" folder under "`%PATROL_HOME%/lib`". All ".hdf" files are installed on all platforms.

The Detection Process

As Hardware Sentry is preloaded by the PATROL Agent, it begins its operations upon the agent startup. Once the Hardware Sentry pre-discovery PSL process has activated the MS_HW_MAIN class, the PATROL Agent spawns the Hardware Sentry discovery PSL process. This PSL process takes two actions: the detection and the environment discovery. Here is a description of this detection process.

- Get the list of available connectors ("*.hdf" files in the `%PATROL_HOME%/lib/MS_HW_hdf` folder)
- For each ".hdf" file found, test the detection criteria (OS type, NT service, processes, SNMP request, etc.)
- Mark the ".hdf" files as "detected" once all its detection criteria is successfully passed. There may be several connectors detected at one time (typically: one connector for the temperatures, voltages, etc., one for the RAID disk controller and one for the non-RAID disk controller)
- Launch the discovery process

Note

To optimize the detection process and gain some time, the detection process is heavily parallelized. All the ".hdf" files are processed simultaneously.

The Discovery Process

The discovery process is launched just after the end of the detection process. It takes the following actions:

- Processes the "Enclosure.Discovery" section of the detected connectors (“.hdf”) that describe the computer model and create the main Hardware Sentry and computer icon (class: MS_HW_ENCLOSURE). Most of other icons (disk controllers, fans, temperatures, etc.) will be created under this computer icon.
- Launches the disk controller discovery that will processes the "DiskController.Discovery" section of each detected “.hdf” file and create the MS_HW_DISKCONTROLLER icons.
- Launches the other discoveries (fans, temperatures, voltages, power supplies, logical disks, physical disks and other devices) that will process the corresponding sections of each detected “.hdf” file and create the corresponding icons.

Note

With a view to optimization, the discovery process is as parallelized as possible. All the independent objects are processed at the same time.

The Collection Process

Once the discovery process is complete, the collection process starts:

- Every two minutes, Hardware Sentry spawns several PSL processes (fanColl, physicalDiskColl, logicalDiskColl, temperatureColl, etc.)
- These PSL processes are responsible for the collection of information about a given device type. For example, fanColl will gather fan information from the different detected hardware information sources, as described in the corresponding “.hdf” Fan.Collect section.
- The PSL processes are "attached" to the main Hardware icon (MS_HW_MAIN class) and not to the corresponding classes and instances. No collection is performed on objects that have been paused.
- When a device is marked as "missing" by the discovery process (i.e. had been discovered and is no longer discovered), the collection process no longer queries the hardware information source, and simply sets the status of the object to alarm.

Monitoring

Monitoring the hardware components with Hardware Sentry is very simple. Once the KM is properly installed, as per the instructions given in the Installation Guide, Hardware Sentry automatically detects all the various hardware components and displays them in the PATROL interface. There is no configuration or "set–up" to be done in order to monitor the hardware of your infrastructure. All you have to do is set/modify thresholds (if required) and set alert actions as per your specific requirements in order to be notified about an error or failure.

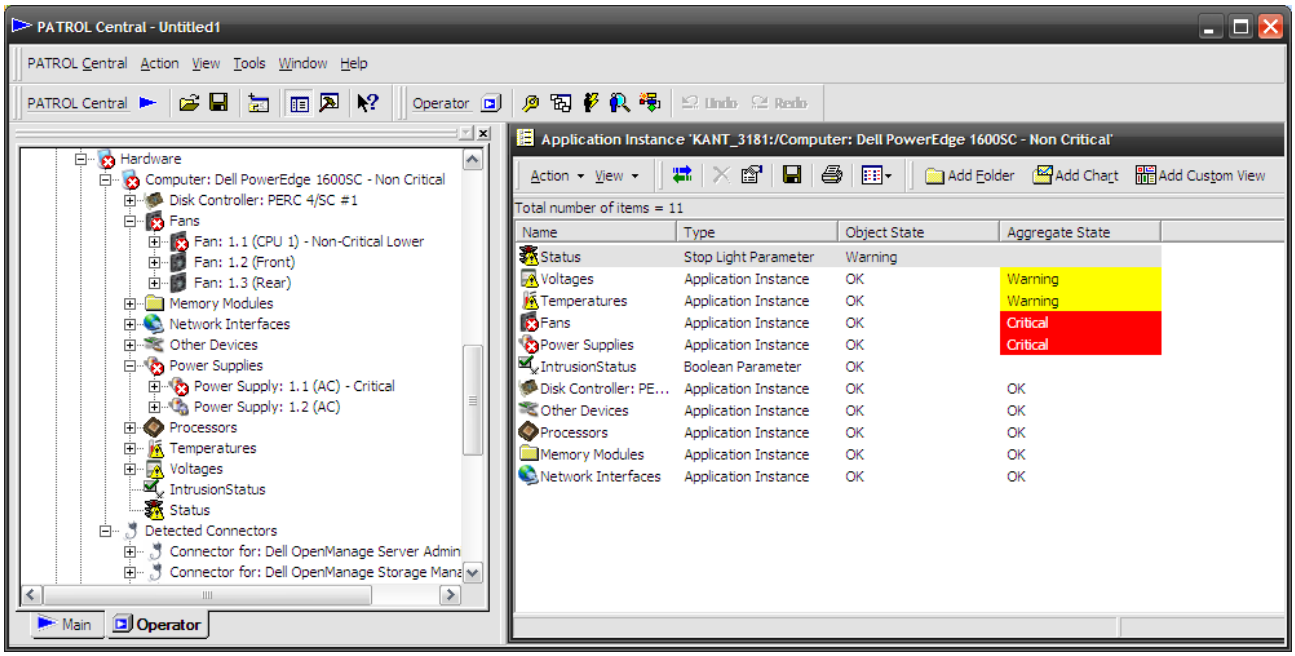
This section gives details about all the components monitored by Hardware Sentry.

The Basics

Automatic detection of hardware components – No configuration required

Hardware Sentry requires no configuration to discover and monitor the hardware components within your BMC Performance Manager environment.

Once the KM is installed and loaded properly after ensuring that all prerequisites have been as described in the Installation Guide (such as installing the manufacturer-specific hardware agents etc.), an icon labeled **Hardware** appears in the Console and the KM discovers all the hardware components of the managed system.



What you can do with the KM…

The easiest way to figure out all that you can do with Hardware Sentry is to investigate the menu commands it offers, and see what these menu commands allow you to do. To illustrate this, the example taken is that of the Dell PowerEdge computer as shown in the picture above.

Menu commands from the Hardware icon

Hardware is the main Hardware icon for each managed system. Right-click on the **Hardware icon > KM Commands >**

The parent menu commands are as follows:

- **KM Settings**: Displays all the command options for different monitoring settings. See table below for description all options offered through *KM Settings*
- **This System's Settings**: Allows you to set system properties and credentials to be used for monitoring. See table below for description of all options offered through *This System's Settings*
- **Add a Remote System to Monitor:** Enables you to monitor another system remotely using either SNMP or WMI/WBEM or Telnet/SSH
- **Instant Hardware Health Report**: Displays an instant hardware health report for the managed system
- **Schedule Hardware Health Reports:** Enables you to schedule automated generation of hardware health reports for all hardware components monitored on the local host (including remote hosts) on an hourly, daily, weekly or monthly basis at given times and days
- **Pause Monitoring**: Enables you to pause the monitoring of the system
- **Resume Monitoring:** Enables you to resume the monitoring that's been paused
- **Trigger a KM Discovery**: Enables you to trigger a full discovery at any time (default discovery once every hour)
- **Reinitialize KM:** Enables you to triggers a complete re-initialization of Hardware Sentry
- **License**: Enables you to enter your license key to activate the Hardware Sentry knowledge module once the trial period expires
- **About**: States basic product information and BMC Software support contact information

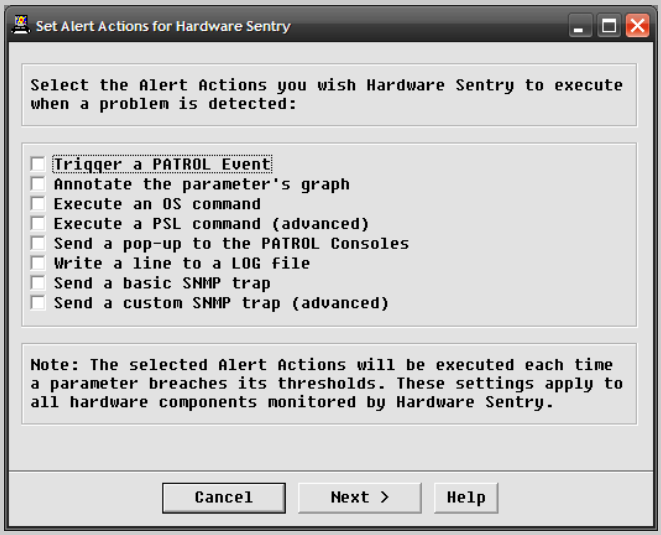
The following two tables give you a quick glimpse of all the options offered through *KM Settings* and *This System's Settings*

KM Settings

Hardware>KM Commands> KM Settings >

Alert Actions…

Enables you to select the Alert Actions i.e. different methods of notifications to be executed by Hardware Sentry when a parameter breaches its threshold


Set Alert Actions for Hardware Sentry
Select the Alert Actions you wish Hardware Sentry to execute when a problem is detected:
Trigger a PATROL Event
Annotate the parameter's graph
Execute an OS command
Execute a PSL command (advanced)
Send a pop-up to the PATROL Consoles
Write a line to a LOG file
Send a basic SNMP trap
Send a custom SNMP trap (advanced)
Note: The selected Alert Actions will be executed each time a parameter breaches its thresholds. These settings apply to all hardware components monitored by Hardware Sentry.
Cancel
Next >
Help

Threshold Mechanism Selection…

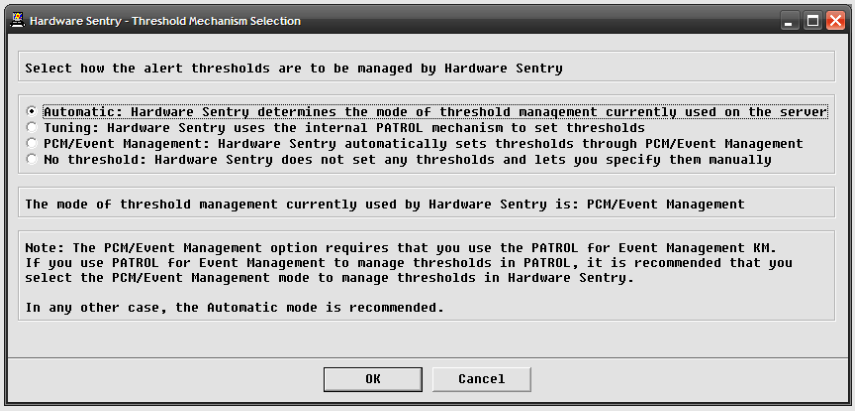
Allows you to select the threshold mechanism:

Automatic (by default): Hardware Sentry determines the mode of threshold management best suited to the system. The different modes are:

Tuning: Hardware Sentry uses the internal PATROL mechanism to set thresholds

PCM/Event Management: Hardware Sentry automatically sets thresholds through PCM/Event Management

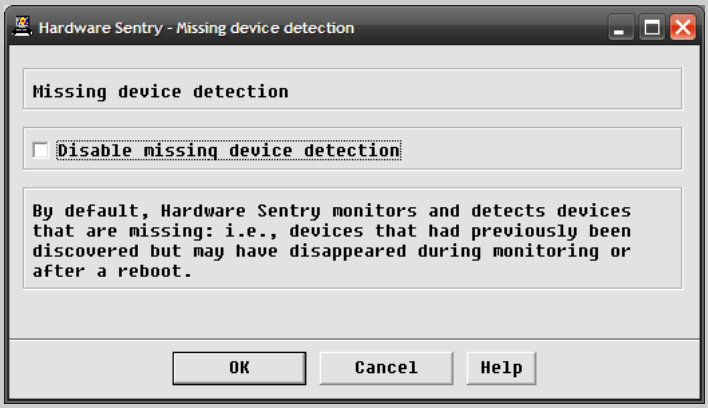
No thresholds: Hardware Sentry does not set any thresholds and lets you specify them manually


Hardware Sentry - Threshold Mechanism Selection
Select how the alert thresholds are to be managed by Hardware Sentry
Automatic: Hardware Sentry determines the mode of threshold management currently used on the server
Tuning: Hardware Sentry uses the internal PATROL mechanism to set thresholds
PCM/Event Management: Hardware Sentry automatically sets thresholds through PCM/Event Management
No threshold: Hardware Sentry does not set any thresholds and lets you specify them manually
The mode of threshold management currently used by Hardware Sentry is: PCM/Event Management
Note: The PCM/Event Management option requires that you use the PATROL for Event Management KM.
If you use PATROL for Event Management to manage thresholds in PATROL, it is recommended that you select the PCM/Event Management mode to manage thresholds in Hardware Sentry.
In any other case, the Automatic mode is recommended.
OK
Cancel

Hardware>KM Commands> KM Settings >

Missing Device Detection…

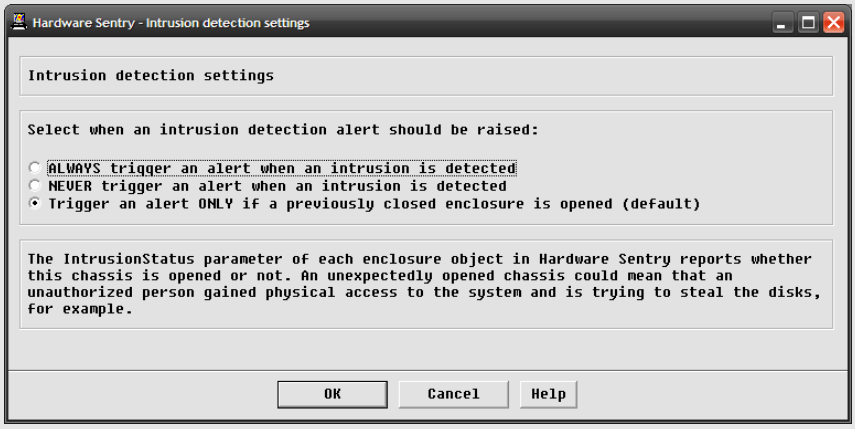
Enables/Disables missing device detection. By default, Hardware Sentry detects "missing devices" i.e. devices previously monitored but which have disappeared during the monitoring or after a reboot or due to some other cause


Hardware Sentry - Missing device detection
Missing device detection
Disable missing device detection
By default, Hardware Sentry monitors and detects devices that are missing: i.e., devices that had previously been discovered but may have disappeared during monitoring or after a reboot.
OK
Cancel
Help

Intrusion Detection Alerts…

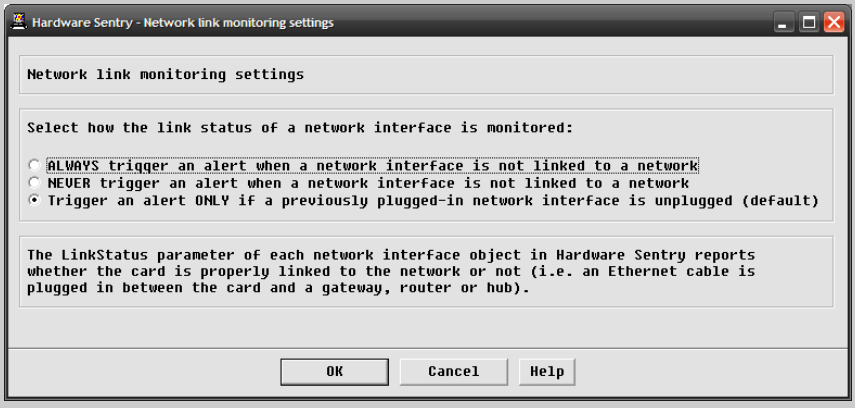
Allows you to decide *when* an intrusion detection alert for the enclosure/ systems chassis should be raised

The *IntrusionStatus* parameter of each enclosure object discovered by Hardware Sentry reports whether or not the chassis has been opened, and triggers an alarm as per user settings.


Hardware Sentry - Intrusion detection settings
Intrusion detection settings
Select when an intrusion detection alert should be raised:
ALWAYS trigger an alert when an intrusion is detected
NEVER trigger an alert when an intrusion is detected
Trigger an alert ONLY if a previously closed enclosure is opened (default)
The IntrusionStatus parameter of each enclosure object in Hardware Sentry reports whether this chassis is opened or not. An unexpectedly opened chassis could mean that an unauthorized person gained physical access to the system and is trying to steal the disks, for example.
OK
Cancel
Help

Network Link Alerts…

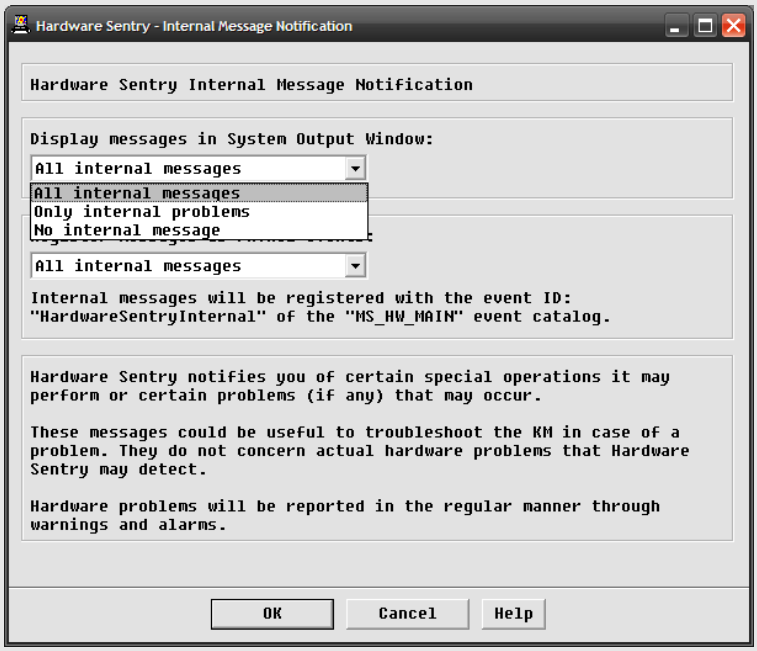
Allows you to choose the monitoring/alert settings for the network link status


Hardware Sentry - Network link monitoring settings
Network link monitoring settings
Select how the link status of a network interface is monitored:
ALWAYS trigger an alert when a network interface is not linked to a network
NEVER trigger an alert when a network interface is not linked to a network
Trigger an alert ONLY if a previously plugged-in network interface is unplugged (default)
The LinkStatus parameter of each network interface object in Hardware Sentry reports whether the card is properly linked to the network or not (i.e. an Ethernet cable is plugged in between the card and a gateway, router or hub).
OK
Cancel
Help

Hardware>KM Commands> KM Settings >

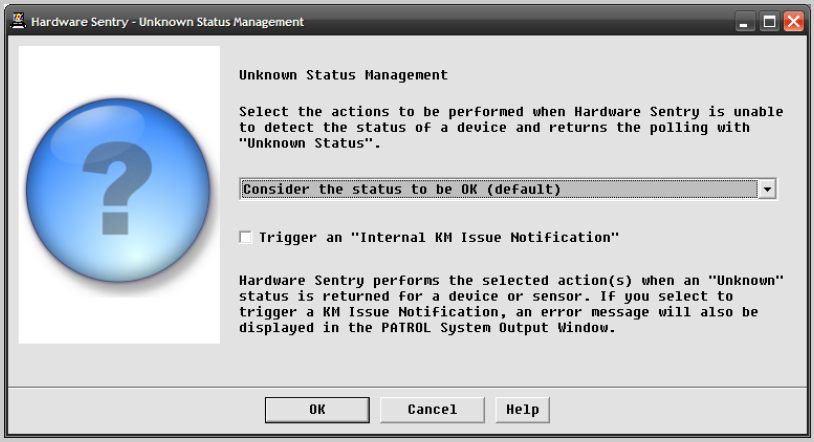
Internal KM Issues Notification…

Allows you to enable/disable and select the type of information messages displayed by Hardware Sentry in the system output window of the PATROL Console


Hardware Sentry - Internal Message Notification
Hardware Sentry Internal Message Notification
Display messages in System Output Window:
All internal messages
All internal messages
Only internal problems
No internal message
All internal messages
Internal messages will be registered with the event ID:
"HardwareSentryInternal" of the "MS_HW_MAIN" event catalog.
Hardware Sentry notifies you of certain special operations it may perform or certain problems (if any) that may occur.
These messages could be useful to troubleshoot the KM in case of a problem. They do not concern actual hardware problems that Hardware Sentry may detect.
Hardware problems will be reported in the regular manner through warnings and alarms.
OK
Cancel
Help

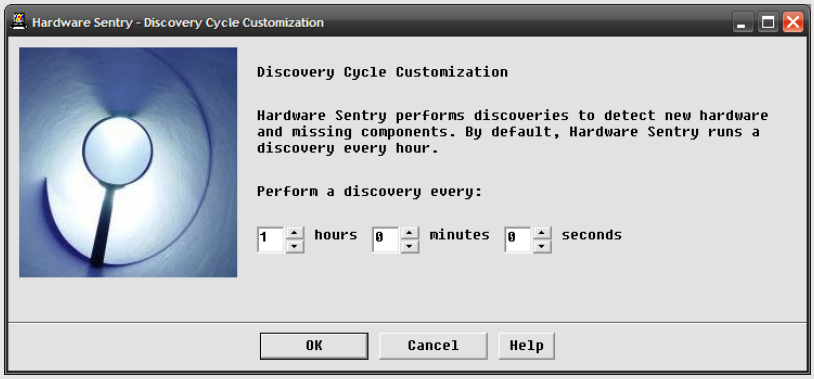
Unknown Status Management…

Allows you to select the actions to be performed if Hardware Sentry returns an “Unknown” status when it is unable to detect a device or sensor


Hardware Sentry - Unknown Status Management
Unknown Status Management
Select the actions to be performed when Hardware Sentry is unable to detect the status of a device and returns the polling with "Unknown Status".
Consider the status to be OK (default)
Trigger an "Internal KM Issue Notification"
Hardware Sentry performs the selected action(s) when an "Unknown" status is returned for a device or sensor. If you select to trigger a KM Issue Notification, an error message will also be displayed in the PATROL System Output Window.
OK
Cancel
Help

Discovery Interval…

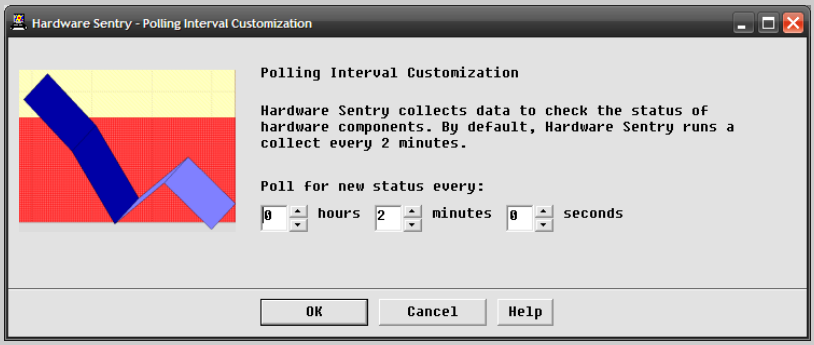
Enables you to customize the discovery cycle. By default, discovery is performed every hour



Hardware>KM Commands> KM Settings >

Polling Interval…

Enables you to customize the polling cycle. By default, the polling interval is done every two minutes


Hardware Sentry - Polling Interval Customization
Polling Interval Customization
Hardware Sentry collects data to check the status of hardware components. By default, Hardware Sentry runs a collect every 2 minutes.
Poll for new status every:
0 hours 2 minutes 0 seconds
OK
Cancel
Help

Additional Settings…

Allows you to:

Restore Device or Sensor Monitoring: Brings up the "Restore Device or Sensor Monitoring" wizard to restore one or several objects after their monitoring has been stopped (if removed)

Display Settings for UNIX console: Gives you the option to turn on the UNIX console mode and modify all object labels to fit the PATROL UNIX Console label size

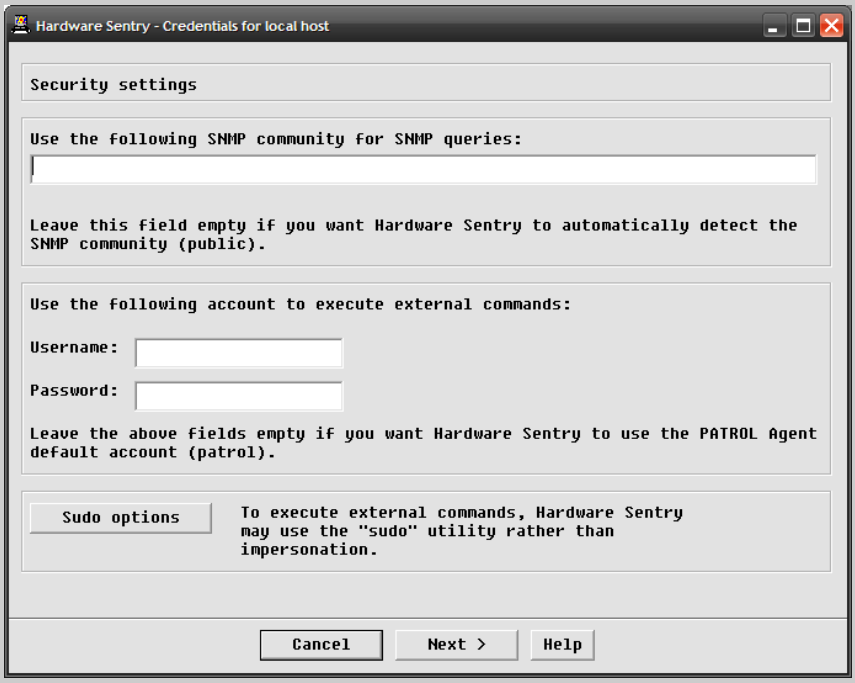
Enable Debug Mode: Activates or deactivates the debug mode. The debug Mode displays debug messages in the PATROL System Output Window or saves it in a file if you enter the file path.

This System's Settings

Hardware > KM Commands > This System's Settings >

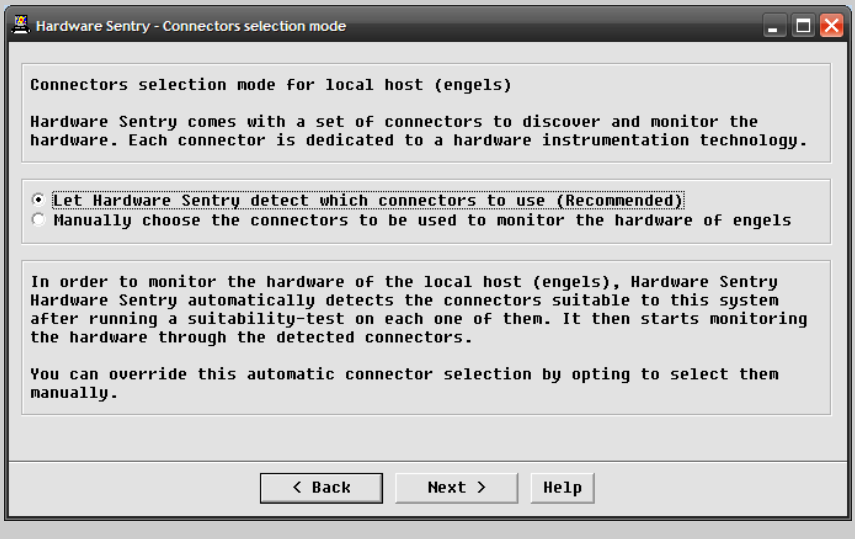
Connection, Credentials and Connectors…

Allows you to set the properties and credentials or the security settings (SNMP string) and/or the account used by Hardware Sentry to launch external commands.


Hardware Sentry - Credentials for local host
Security settings
Use the following SNMP community for SNMP queries:
Leave this field empty if you want Hardware Sentry to automatically detect the SNMP community (public).
Use the following account to execute external commands:
Username:
Password:
Leave the above fields empty if you want Hardware Sentry to use the PATROL Agent default account (patrol).
Sudo options
To execute external commands, Hardware Sentry may use the "sudo" utility rather than impersonation.
Cancel
Next >
Help

The next step allows you to set/modify the way connectors are selected: By Hardware Sentry (default) or by the user (manual)

Hardware Sentry uses a set of connectors to discover and monitor the various hardware components. Each *Connector* is dedicated to a hardware instrumentation technology.

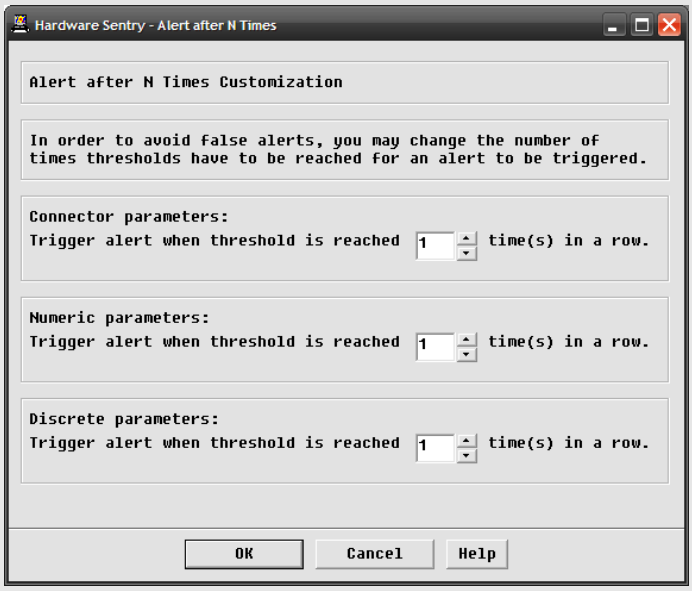

Hardware Sentry - Connectors selection mode
Connectors selection mode for local host (engels)
Hardware Sentry comes with a set of connectors to discover and monitor the hardware. Each connector is dedicated to a hardware instrumentation technology.
Let Hardware Sentry detect which connectors to use (Recommended)
Manually choose the connectors to be used to monitor the hardware of engels
In order to monitor the hardware of the local host (engels), Hardware Sentry Hardware Sentry automatically detects the connectors suitable to this system after running a suitability-test on each one of them. It then starts monitoring the hardware through the detected connectors.
You can override this automatic connector selection by opting to select them manually.
< Back
Next >
Help

Hardware > KM Commands > This System's Settings >

Alert After N Times...

Allows you to customize the alert thresholds mechanism in order to avoid false alerts.

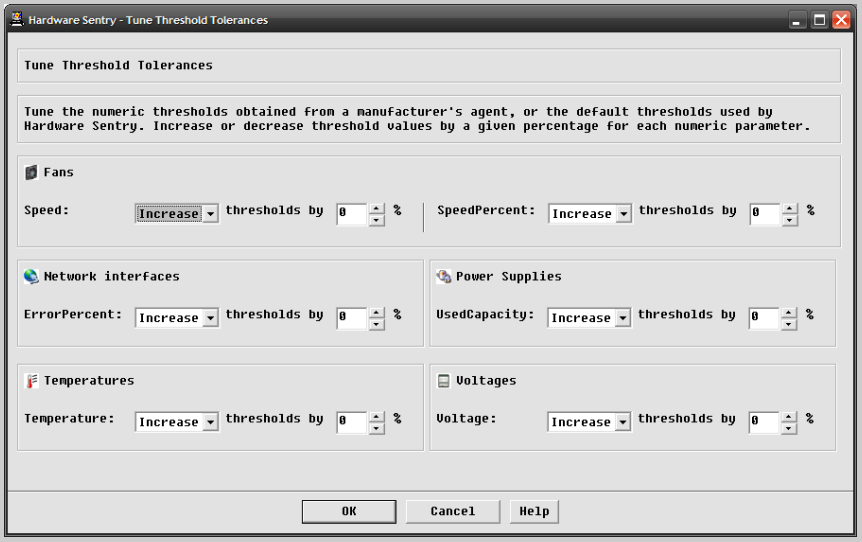
You can set/change the number of times thresholds can be breached before an alert is triggered.


Hardware Sentry - Alert after N Times
Alert after N Times Customization
In order to avoid false alerts, you may change the number of times thresholds have to be reached for an alert to be triggered.
Connector parameters:
Trigger alert when threshold is reached 1 time(s) in a row.
Numeric parameters:
Trigger alert when threshold is reached 1 time(s) in a row.
Discrete parameters:
Trigger alert when threshold is reached 1 time(s) in a row.
OK
Cancel
Help

Tune Threshold Tolerances...

Allows you to tune the numeric thresholds obtained from a manufacturer's agent, or the default thresholds used by Hardware Sentry.

You can increase or decrease threshold values by a given percentage for each numeric parameter


Hardware Sentry - Tune Threshold Tolerances
Tune Threshold Tolerances
Tune the numeric thresholds obtained from a manufacturer's agent, or the default thresholds used by Hardware Sentry. Increase or decrease threshold values by a given percentage for each numeric parameter.
Fans
Speed: Increase thresholds by 0 %
SpeedPercent: Increase thresholds by 0 %
Network interfaces
ErrorPercent: Increase thresholds by 0 %
Power Supplies
UsedCapacity: Increase thresholds by 0 %
Temperatures
Temperature: Increase thresholds by 0 %
Voltages
Voltage: Increase thresholds by 0 %
OK
Cancel
Help

Remove this System...

Enables you to remove a remote system added to the monitoring environment

Remove a system
Remove the remote hardware monitoring of nieztsche.
Are you sure you wish to remove the hardware monitoring of nieztsche?
Yes
No

Device specific KM commands

The KM commands that are offered by right-clicking on a monitored hardware component/device are:

- **Instant Hardware Health Report…:** Displays a report about the health of a device.
- **Modify Alert Thresholds**…: Enables you to modify alert thresholds
- **Pause Monitoring…**: Enables you to pause the monitoring of the hardware component
- **Resume Monitoring…**: Enables you to resume the monitoring that had previously been paused
- **Remove…**: Allows you to remove the object from the monitoring environment
- **Refresh Parameters…**: Allows you to refresh the parameters of the monitored object
- **Acknowledge "X" Alert/Acknowledge Alert and Reset Error Count** etc.: Depending on the component/device monitored and the type of system it is monitored on, there may be certain additional commands to acknowledge alerts, or acknowledge alerts and reset the error count etc.

  For instance, in the case of *Network Interfaces* there is an additional command: **Acknowledge LinkStatus Alert**

Device-container KM commands

Hardware Sentry creates "containers" for each device.

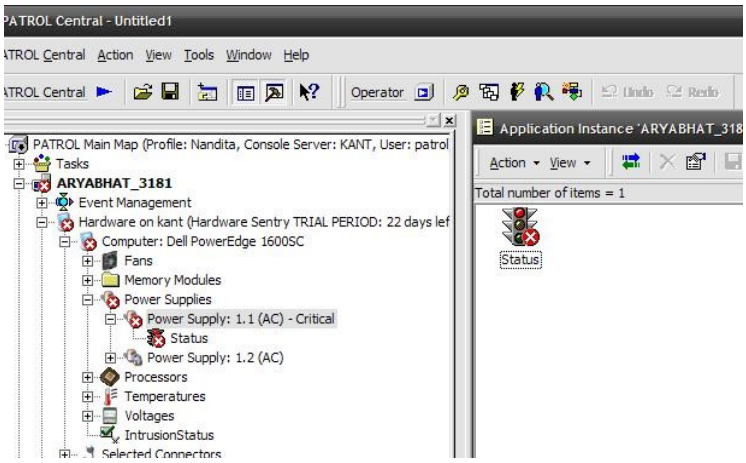
For instance, an icon is created for *Network Interfaces* under which all actual network interfaces discovered will be grouped.

Each such "device container" has commands such as: **Pause Monitoring; Resume Monitoring; Remove; Refresh Parameters** whose actions are applicable to *all* objects under it.

Note

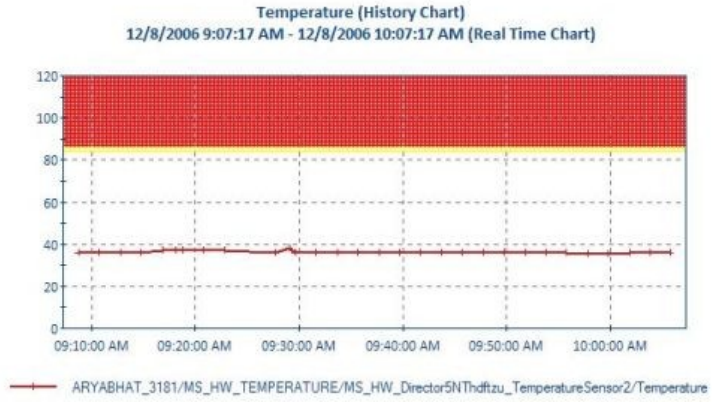
The Reference Guide lists all the menu commands for each application class along with parameter details.

Monitoring Temperatures, Fans, Voltages and Power-Supplies



Hardware Sentry automatically detects the information sources available on the monitored computer and displays the hardware information provided by those sources in the PATROL Consoles in the corresponding container.

If a hardware information source provides useful data about temperatures, fans, voltages or power-supplies, an icon is automatically created for each sensor found in the system as well as one or more parameters.



For each displayed sensor, one or more graphs are built with the data polled every two minutes. These graphs can be viewed by double-clicking the parameter under the corresponding icon in the PATROL Console.

The location or the type of the sensor may appear in the icon label if this information is available as well.

Depending on the platform and sensors, and if possible, alert thresholds are automatically set by Hardware Sentry. When the parameter value reaches these thresholds, the parameter triggers a warning or an alarm and this alert is sent by the PATROL Console to the operators and administrators.

Note

If a device appears to be missing, the *Status* parameter will trigger an alert if necessary.

Note

The parameters discovered depend on the server type. All parameters may not be discovered on all servers. Please refer to the Connector and Platform details in the Reference guide to see which parameters are displayed for the different servers, and for details on the available menu commands, please see the Application Classes section in the same guide This. documentation is also available in an online format from with the product as well as in the Hardware Sentry Online Technical Library accessible on the Sentry Software website.

Fans

To avoid overheating, fans are installed on critical devices such as: processors, power supplies, etc.). If a cooling system is not present, an overheated system can throttle the speed of processors and cause slow-downs or ultimately cause shut-downs. Monitoring fans is important since they ensure maintaining the right temperatures for optimal functioning of the system.

Depending on the information available, the *Speed* and/or *SpeedPercent* and/or *Status* parameters will be displayed for each detected fan device:

- The *Speed* parameter represents the speed of the corresponding fan in rotations/minute. An alert is triggered if the fan speed is too low for proper functioning.
- The *SpeedPercent* parameter represents the speed of the corresponding fan in percentage of its maximal speed. An alert is triggered if the fan speed is too low for proper cooling.
- The *Status* parameter represents the current status of the fan. An alert is triggered if the fan stops spinning or does not spin fast enough.

Temperatures

As with any electronic device, chips and other components of a computer stop working when overheated. Overheating could result in several unrecoverable errors, crashes and even hardware damage. Temperatures may rise too high when a device is abnormally overloaded; a fan is not working properly or when the ambient temperature is too hot. Monitoring the temperatures of the critical devices of your system allows you to take preventive action and avoid a crash from overheating.

Depending on the information available, the *Temperature* and/or *Status* parameters will be displayed for each detected temperature sensor:

- The *Temperature* parameter represents the current temperature reading in Celsius degrees (°C). An alert is triggered if the temperature rises too high.
- The *Status* parameter represents the current status of the temperature. An alert is triggered if the temperature gets too high.

Power supply

Power supply is the component that transforms the AC Line into electric power needed by the computer. Therefore the power supply is a highly critical device of a computer that should never fail. Due to this, most vendors build servers with redundant power supplies. Monitoring power supplies allows the operators to be alerted when a power supply fails, or in some cases, even when a power supply is overloaded.

Depending on the available information, the *UsedCapacity* and/or *Status* parameters will be displayed for each power supply or power unit device:

- The *UsedCapacity* parameter represents the power currently in use as a percentage. An alert is triggered when the power supply's maximum power output is reached.
- The *Status* parameter represents the current status of the power supply. An alert is triggered if an error occurs with the power supply.

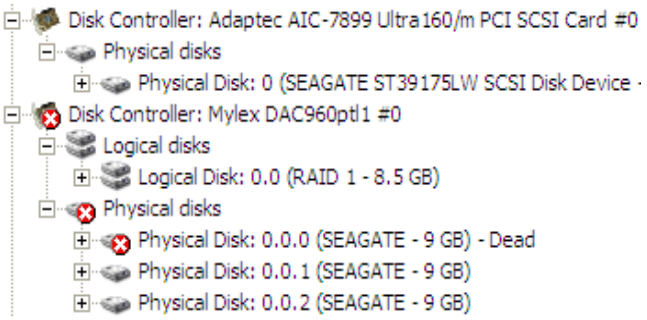
Voltages

Power supplies convert the AC line power into voltages and currents needed by the motherboard of the computer. The stability of the motherboard (and therefore that of the overall computer) strongly depends on this power converter. Voltages that are too low or too high may lead to unpredictable system crashes. Monitoring the value of the different voltages needed by the motherboard will help in detecting system instability.

Depending on the available information, the *Voltage* and/or *Status* parameters will be displayed for each voltage sensor on the motherboard:

- The *Voltage* parameter represents the voltage output in milliVolts (mV). An alert is triggered if the voltage goes out of the range.
- The *Status* parameter represents the current status of the voltage. An alert is triggered if the voltage output is too low for proper functioning.

Monitoring Disks


Disk Controller: Adaptec AIC-7899 Ultra160/m PCI SCSI Card #0
Physical disks
Physical Disk: 0 (SEAGATE ST39175LW SCSI Disk Device
Disk Controller: Mylex DAC960ptl1 #0
Logical disks
Logical Disk: 0.0 (RAID 1 - 8.5 GB)
Physical disks
Physical Disk: 0.0.0 (SEAGATE - 9 GB) - Dead
Physical Disk: 0.0.1 (SEAGATE - 9 GB)
Physical Disk: 0.0.2 (SEAGATE - 9 GB)

Hardware Sentry automatically detects the information sources available on the monitored computer and displays the hardware information provided by those sources in the PATROL Consoles in the corresponding container.

If at least one hardware information source provides useful data about the storage in the computer, an icon will be created for each storage-related device in the PATROL Console: disk controllers, physical disks and logical disks.

Physical and logical disks icons are created below the disk controller icons they are attached too. Each icon is labeled with a description of the device: ID, size, vendor, role, etc.

Note

If a device appears to be missing, the *Status* parameter will trigger an alert if necessary.

Note

The parameters discovered depend on the server type. All parameters may not be discovered on all servers. Please refer to the Connector and Platform details in the Reference guide to see which parameters are displayed for the different servers, and for details on the available menu commands, please see the Application Classes section in the same guide This. documentation is also available in an online format from with the product as well as in the Hardware Sentry Online Technical Library accessible on the Sentry Software website.

Disk controllers

A disk controller is a card inside a computer that connects one or several physical disk drives to this computer. Some intelligent disk controllers (such as RAID controllers) manage several physical disks as a single logical disk which is the only disk exposed to the operating system. Monitoring both physical and logical disks is essential to ensure that storage is available.

The purpose of the Disk Controller instance is to act as a container for Logical Disks and Physical Disks monitoring, and symbolize the way hard drives are setup on the platform. In addition, some information regarding the Disk Controllers, like their brand, model or driver version, is displayed in the InfoBox.

Depending on the information available, the *BatteryStatus* and *ControllerStatus* parameters will be displayed.

- The *BatteryStatus* parameter triggers an alert to predict that the disk controller battery will be unable to support the controller in the event of a power failure.
- The *ControllerStatus* parameter displays the status of the disk controller.

Note

If a controller goes missing, all its disk dependencies will be missing as well.

Physical Disks

Physical disks must be monitored to avoid loss of data, unavailability and performance degradation. When available, S.M.A.R.T. technology is used to predict a disk failure.

Depending on the available information, the *PredictedFailure*, *ErrorCount* and/or *Status* parameters will be displayed for each discovered physical disk:

- The *PredictedFailure* parameter uses S.M.A.R.T. technology to predict physical disk failures. An alert will be triggered if a breakdown of a Physical Disk is predicted.
- The *ErrorCount* parameter is incremented each time an error occurs on this physical disk. An alert is raised from the first detected error. The operator can reset the counter and clear the alert through a menu command in the PATROL Console.
- The *Status* parameter represents the current status of the physical disk. An alert is triggered if the physical disk is not available for proper operation.

Logical Disks

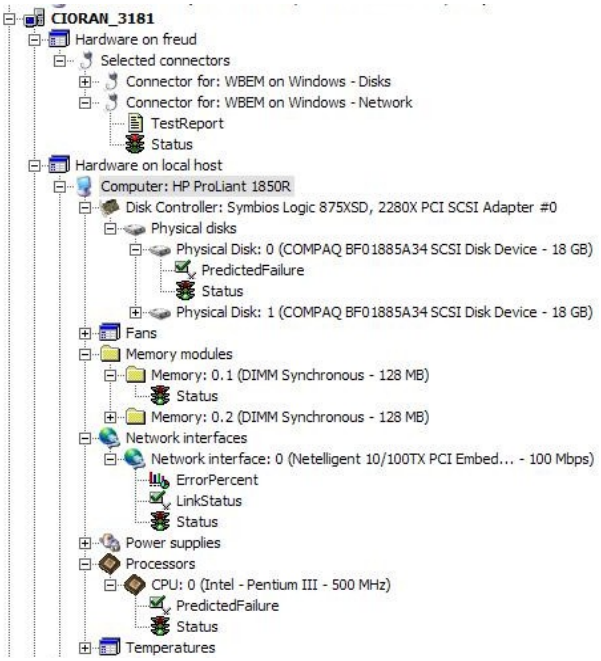
RAID or advanced disk controllers expose several physical disks as a single logical disk to the operating system. The status of a logical disk typically corresponds to the status of a RAID array (on-line, degraded, rebuilding, etc.). The *Status* parameter is displayed for each logical disk discovered.

- The *Status* parameter represents the current status of the logical disk. An alert is triggered when the logical disk is not fully operational (degraded, rebuilding, etc.) or not available at all.

Note

For non-RAID disk controllers (as most of IDE controllers, for example), no logical disk will be displayed.

Monitoring Processors, Memory modules and Network Interfaces



Hardware Sentry automatically detects the information sources available on the monitored computer and displays the hardware information provided by those sources in the PATROL Consoles in the corresponding container.

If at least one hardware information source provides useful data about the most critical non-storage devices in the computer, an icon will be created for each device in the PATROL Console: processors, memory modules and network interfaces.

Processors, memory modules and network interfaces icons are created under a computer icon. Each icon is labeled with a description of the device: ID, size, vendor, role, etc.

Note

If a device appears to be missing, the “Status” parameter will trigger an alert if necessary.

Note

The parameters discovered depend on the server type. All parameters may not be discovered on all servers. Please refer to the Connector and Platform details in the Reference guide to see which parameters are displayed for the different servers, and for details on the available menu commands, please see the Application Classes section in the same guide This. documentation is also available in an online format from with the product as well as in the Hardware Sentry Online Technical Library accessible on the Sentry Software website.

Processors

Processors (also called CPU, Central Processing Unit) are undoubtedly very critical devices within a computer. While a processor fault may often lead to a system crash without a chance for a monitoring tool to catch the error, it is still helpful to monitor the processors of servers.

In case of a system crash due to a fault in the processor, the system reboots automatically. The reboot is either triggered by the operating system or by the motherboard itself. If a processor is no longer functioning, it is automatically disabled by the BIOS and, if there is one other processor left, the operating system starts with one processor less.

Hardware Sentry monitors each processor and verifies if it is present and running. If a processor is missing upon a reboot, Hardware Sentry triggers an alert.

On some recent or high-end servers, processors are able to correct some operation errors by themselves (like the ECC memory). If this information is available, it is shown in the PATROL Console by Hardware Sentry. In addition, if the processor is able to predict a failure, this information will be monitored by Hardware Sentry and shown in the PATROL Console.

Depending on the information available, the *Status* and/or *CorrectedErrorCount* and/or *PredictedFailure* parameters will be displayed for each discovered processor (CPU):

- The *Status* parameter represents the current status of the processor. An alert is triggered if the processor is not available for proper operation (missing, disable by the BIOS due to a POST error, etc.).
- The *PredictedFailure* parameter reports the predicted failure analysis performed by the processor itself. This information is based on the rate of corrected errors.
- The *CorrectedErrorCount* parameter represents the number of errors that have been automatically corrected by the processor. This information can be very useful to predict a failure in the near future.

Memory Modules

The main memory of a computer is actually as critical as the processors since almost all processor operations deal with memory. A single memory fault could lead to a severe computer crash with potential data corruption. On servers, the memory modules (the devices where the memory data is actually stored) often include auto-correction features (ECC), and sometimes even better: RAID5-like memory configuration. These features and configurations allow the memory modules to report statistics on failures, to predict failures, to hot-replace a memory module upon failure, etc.

Depending on the available information and the features provided by the motherboard and the memory modules, the *ErrorCount* and/or *PredictedFailure* and/or *Status* parameters will be displayed for each discovered memory module:

- The *ErrorCount* parameter reports the number of errors detected by the memory module and then corrected. A steadily growing value means that the memory module is not reliable and that it could encounter errors that it is unable to correct, which could then lead to a system crash.
- The *ErrorStatus* parameter deals with the same kind of errors as the *ErrorCount* parameter but in a more accurate manner. The only difference is that, once a specified threshold is reached, an alert is triggered, so the number of errors will not actually be displayed. It is unnecessary to set an error threshold as these thresholds are calculated and set by the systems hardware agent.
- The *PredictedFailure* parameter reported by the memory modules predicts failure by analyzing the trend of the number of detected/corrected errors (thanks to the ECC technology). If this parameter goes into alarm, replacement of the faulty module is highly recommended.

- The *Status* parameter represents the current status of the memory module. An alert is triggered if the memory module reports a failure (in a RAID5-like configuration) or if it goes missing after a computer reboot.

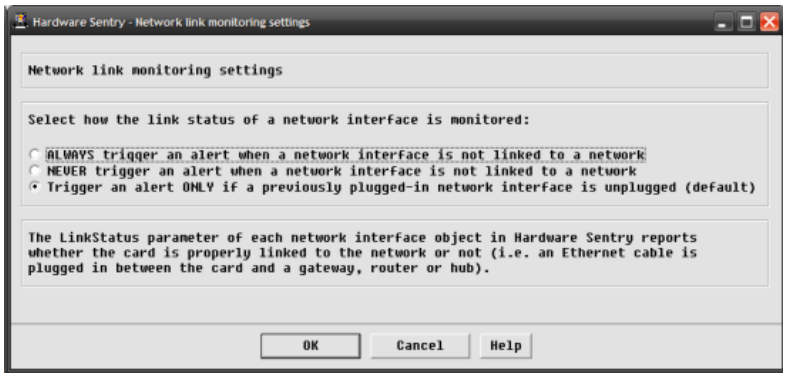
Network Interfaces

Network interfaces are devices that serve as a common interface for various other devices within a local area network (LAN), or as an interface to allow networked computers to connect to an outside network. It is therefore essential to make sure these devices are linked to the network and function properly. For each network interface discovered, the *Status, ErrorPercent* and/or *LinkStatus* parameters are displayed:

The *Status* parameter represents the current status of the network interface. An alert is triggered when the network interface does not respond.

- The *ErrorPercent* parameter gives the percentage of transmitted and received packets that were in error (due to low-level protocol error or physical media problems). A warning is raised when this percentage goes above 10% and an alarm when above 30%. A frequent high error percentage implies there is a serious problem with the cable or the interface.
- The *LinkStatus* parameter shows the current status of the network interface to the network (i.e. whether or not it is plugged-in). By default, Hardware Sentry will trigger a warning if a network interface previously connected to the network is now unplugged. However, it will not trigger an alert for network interfaces that were never connected.

To change this setting, right-click the main Hardware icon and select **KM Commands** > **KM Settings** > **Network Link Alerts**... This will display the dialog box shown below:


Hardware Sentry - Network link monitoring settings
Network link monitoring settings
Select how the link status of a network interface is monitored:
ALWAYS trigger an alert when a network interface is not linked to a network
NEVER trigger an alert when a network interface is not linked to a network
Trigger an alert ONLY if a previously plugged-in network interface is unplugged (default)
The LinkStatus parameter of each network interface object in Hardware Sentry reports whether the card is properly linked to the network or not (i.e. an Ethernet cable is plugged in between the card and a gateway, router or hub).
OK
Cancel
Help

Three options are possible:

- ALWAYS trigger an alert when a network interface is not linked to a network: if a network card is unplugged, Hardware Sentry will trigger an alert no matter what.
- NEVER trigger an alert when a network interface is not linked to a network: this basically turns off the monitoring of the network link.
- Trigger an alert ONLY if the previously plugged-in network interface is unplugged (default).

Monitoring Remote Systems

Hardware Sentry is able to monitor the hardware of a system remotely through the network. The purpose of this function is not to monitor all servers from one agent, but to be able to monitor devices on which one cannot install a PATROL Agent, like the chassis of blade servers, tape libraries, etc.

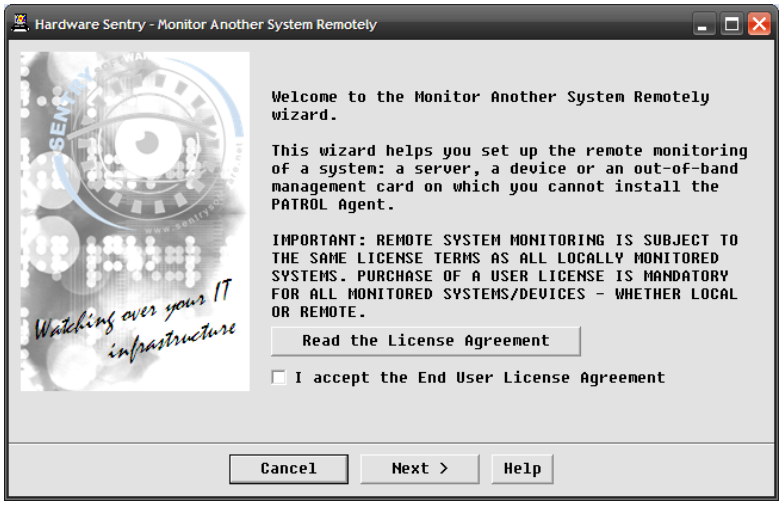
Hardware Sentry monitors systems remotely through the SNMP, SSH, Telnet and WBEM/WMI protocols. This means that only SNMP, SSH, Telnet and WBEM/WMI based connectors will function properly for remote devices.

Note

Configuring Hardware Sentry to monitor another system remotely does not prevent it from monitoring the hardware of the local host where the KM is running. Once configured to monitor another system remotely, the KM will show two icons side-by-side in the PATROL Console: “Hardware on local host” and “Hardware on <RemoteSystem>”.

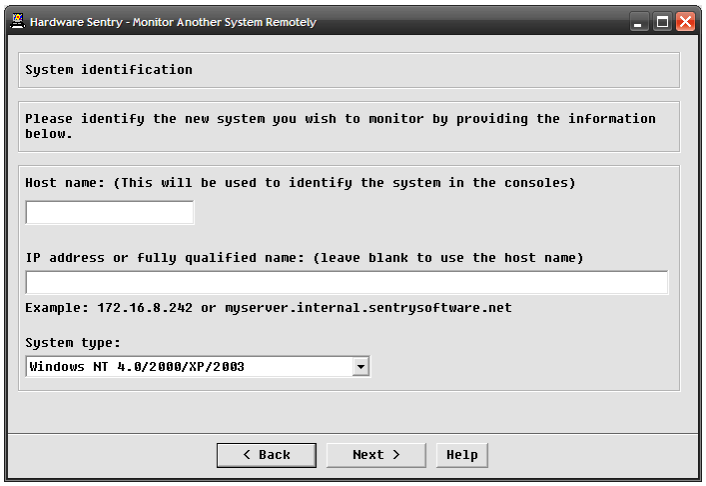
How to monitor a device remotely

1. Right click on the local host’s **Hardware icon > KM Commands > Add a Remote System to Monitor**


Hardware Sentry - Monitor Another System Remotely
Watching over your IT infrastructure
Welcome to the Monitor Another System Remotely wizard.
This wizard helps you set up the remote monitoring of a system: a server, a device or an out-of-band management card on which you cannot install the PATROL Agent.
IMPORTANT: REMOTE SYSTEM MONITORING IS SUBJECT TO THE SAME LICENSE TERMS AS ALL LOCALLY MONITORED SYSTEMS. PURCHASE OF A USER LICENSE IS MANDATORY FOR ALL MONITORED SYSTEMS/DEVICES - WHETHER LOCAL OR REMOTE.
Read the License Agreement
I accept the End User License Agreement
Cancel
Next >
Help

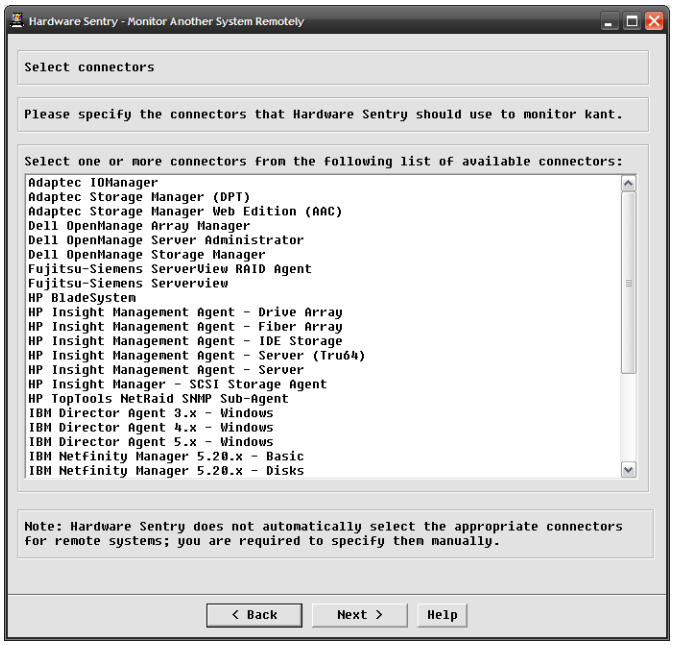
2. Read the License agreement, accept it and click on **Next**.

3. Identify the system you want to monitor remotely and click **Next**.


Hardware Sentry - Monitor Another System Remotely
System identification
Please identify the new system you wish to monitor by providing the information below.
Host name: (This will be used to identify the system in the consoles)
IP address or fully qualified name: (leave blank to use the host name)
Example: 172.16.8.242 or myserver.internal.sentrysoftware.net
System type:
Windows NT 4.0/2000/XP/2003
< Back
Next >
Help

- **Host name**: Enter the host name of the remote system
- **IP address or fully qualified name**: Leave this field blank if you specify the host name above
- **System type**: Select a platform from the drop down list to specify the system type. The options are: OpenVMS, HP Tru64 UNIX, HP-UX, IBM AIX, Linux (Red Hat, SuSe), Out-of-band monitoring, Storage, Sun Solaris, Windows NT 4.0/2000/XP/2003

4. Select the connectors Hardware Sentry should use to monitor the remote system/device.


Hardware Sentry - Monitor Another System Remotely
Select connectors
Please specify the connectors that Hardware Sentry should use to monitor kant.
Select one or more connectors from the following list of available connectors:
Adaptec IOManager
Adaptec Storage Manager (DPT)
Adaptec Storage Manager Web Edition (AAC)
Dell OpenManage Array Manager
Dell OpenManage Server Administrator
Dell OpenManage Storage Manager
Fujitsu-Siemens ServerView RAID Agent
Fujitsu-Siemens Serverview
HP BladeSystem
HP Insight Management Agent - Drive Array
HP Insight Management Agent - Fiber Array
HP Insight Management Agent - IDE Storage
HP Insight Management Agent - Server (Tru64)
HP Insight Management Agent - Server
HP Insight Manager - SCSI Storage Agent
HP TopTools NetRaid SNMP Sub-Agent
IBM Director Agent 3.x - Windows
IBM Director Agent 4.x - Windows
IBM Director Agent 5.x - Windows
IBM Netfinity Manager 5.20.x - Basic
IBM Netfinity Manager 5.20.x - Disks
Note: Hardware Sentry does not automatically select the appropriate connectors for remote systems; you are required to specify them manually.
< Back
Next >
Help

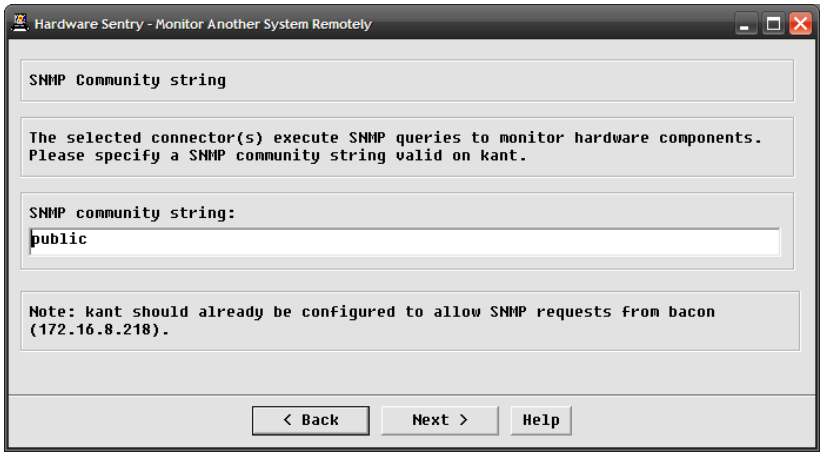
The connectors displayed depend on the system-type specified in the previous step.

5. Select the appropriate connectors and click **Next**.

Note

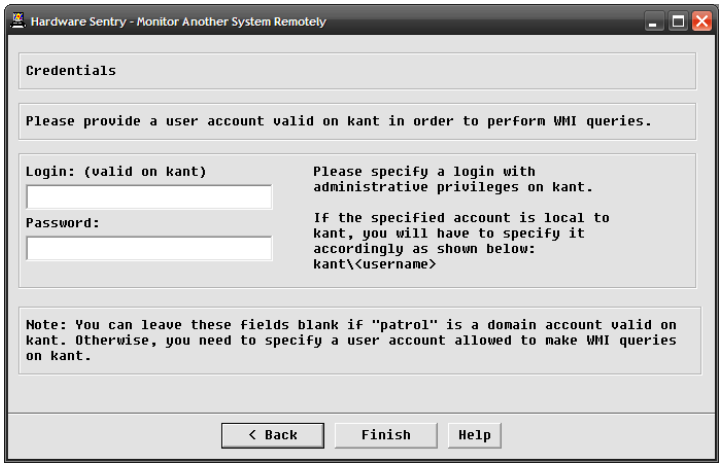
The following panels depend on the system type of the remote element and the protocols used to connect to it. For information on which connectors are suitable for each system, please refer to the Connector and Platform Reference Table in the Reference Guide.

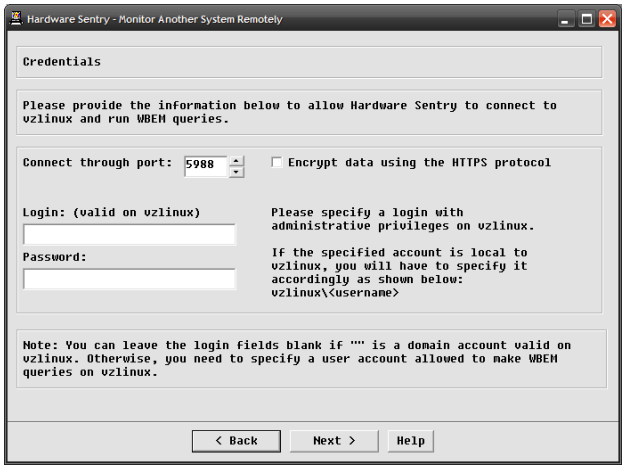
If the connectors selected use SNMP, this panel will appear:


Hardware Sentry - Monitor Another System Remotely
SNMP Community string
The selected connector(s) execute SNMP queries to monitor hardware components.
Please specify a SNMP community string valid on kant.
SNMP community string:
public
Note: kant should already be configured to allow SNMP requests from bacon (172.16.8.218).
< Back
Next >
Help

- **SNMP community**: Enter the SNMP community string and click **Next**.

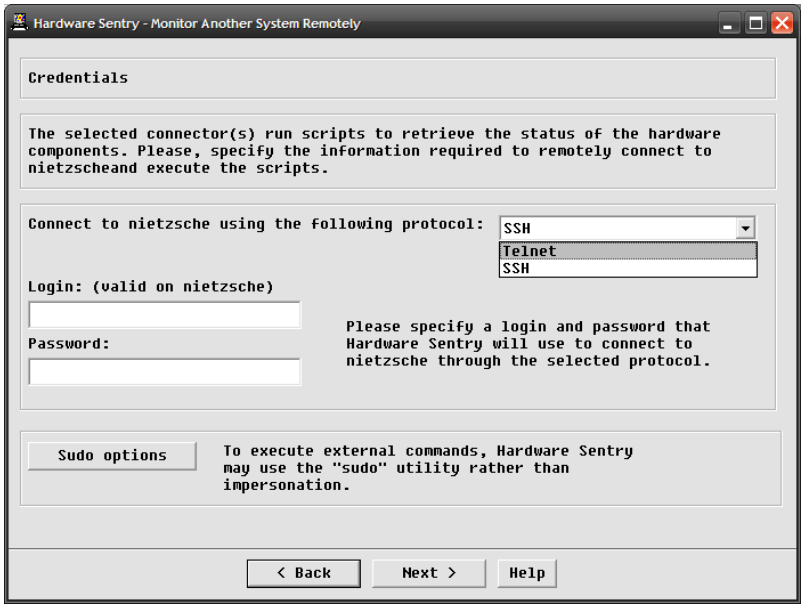
If the connectors selected use WMI or WBEM, the following panels will ask for connection credentials:


Hardware Sentry - Monitor Another System Remotely
Credentials
Please provide a user account valid on kant in order to perform WMI queries.
Login: (valid on kant)
Password:
Please specify a login with administrative privileges on kant.
If the specified account is local to kant, you will have to specify it accordingly as shown below: kant\<username>
Note: You can leave these fields blank if "patrol" is a domain account valid on kant. Otherwise, you need to specify a user account allowed to make WMI queries on kant.
< Back
Finish
Help

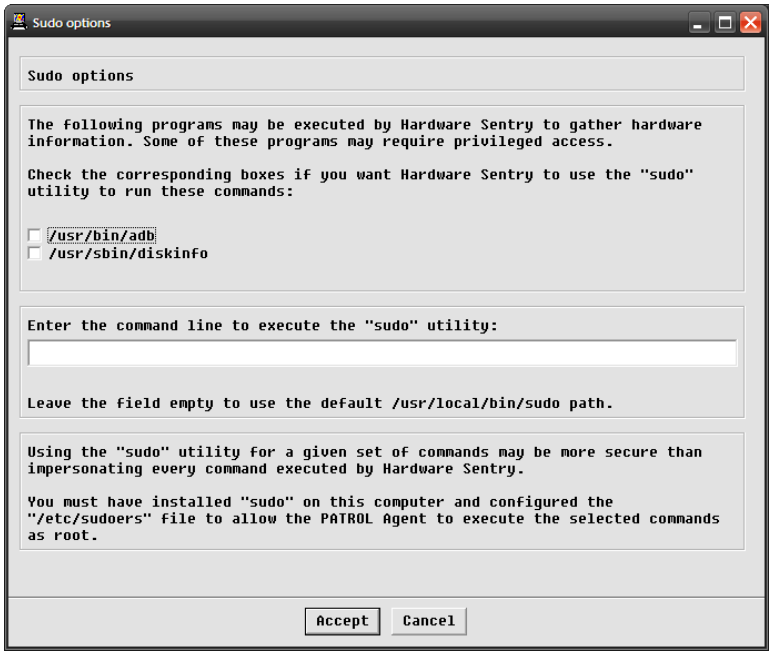

Hardware Sentry - Monitor Another System Remotely
Credentials
Please provide the information below to allow Hardware Sentry to connect to vzlinux and run WBEM queries.
Connect through port: 5988
Encrypt data using the HTTPS protocol
Login: (valid on vzlinux)
Password:
Please specify a login with administrative privileges on vzlinux.
If the specified account is local to vzlinux, you will have to specify it accordingly as shown below: vzlinux\<username>
Note: You can leave the login fields blank if "" is a domain account valid on vzlinux. Otherwise, you need to specify a user account allowed to make WBEM queries on vzlinux.
< Back
Next >
Help

- **WMI/WBEM credentials**: Enter the WMI/WBEM credentials and click **Finish/Next**.

If the connectors selected require Telnet or SSH to connect to the remote element, the following panel will appear.


Hardware Sentry - Monitor Another System Remotely
Credentials
The selected connector(s) run scripts to retrieve the status of the hardware components. Please, specify the information required to remotely connect to nietzscheand execute the scripts.
Connect to nietzsche using the following protocol:
SSH
Telnet
SSH
Login: (valid on nietzsche)
Password:
Please specify a login and password that Hardware Sentry will use to connect to nietzsche through the selected protocol.
Sudo options
To execute external commands, Hardware Sentry may use the "sudo" utility rather than impersonation.
< Back
Next >
Help

- **Telnet/SSH**: Select either **Telnet** or **SSH** and enter the credentials required to execute the protocols and click **Next**.
- **Sudo options**: On UNIX/Linux platforms, you have the option of permitting Hardware Sentry to use the sudo utility to execute external commands using root.


Sudo options
Sudo options
The following programs may be executed by Hardware Sentry to gather hardware information. Some of these programs may require privileged access.
Check the corresponding boxes if you want Hardware Sentry to use the "sudo" utility to run these commands:
/usr/bin/adb
/usr/sbin/diskinfo
Enter the command line to execute the "sudo" utility:
Leave the field empty to use the default /usr/local/bin/sudo path.
Using the "sudo" utility for a given set of commands may be more secure than impersonating every command executed by Hardware Sentry.
You must have installed "sudo" on this computer and configured the "/etc/sudoers" file to allow the PATROL Agent to execute the selected commands as root.
Accept
Cancel

Select the command/s, enter the command line to execute the sudo utility and click **Accept**.

Final step in the remote monitoring wizard common to all platforms/systems

Hardware Sentry - Force Discovery
Perform a new hardware discovery
A full discovery needs to be triggered by Hardware Sentry to add the new host and perform a new platform detection to figure out the environement and list the harwdare components.
Click the Finish button to apply the add the remote monitoring of bacon and perform a full discovery.
< Back
Finish
Help

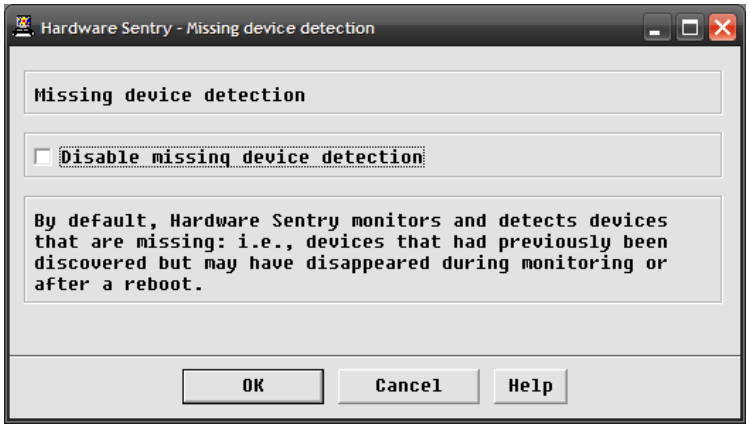
Click **Finish** and Hardware Sentry will perform a new full discovery to detect this new remote system.

The **Hardware** icon for the local host will change to **Hardware on localhost** and an icon labeled **Hardware on <remotehostname>** will appear. This represents the device you are now monitoring remotely, along with icons for all of the detected parameters of this remote device/system.

Detecting Missing Devices

The missing device detection mechanism of Hardware Sentry alerts operators when a device that was previously detected in the system is no longer found.

This mechanism is very useful when, for example, a non-redundant physical disk does not restart during a system reboot and therefore is no longer seen by the operating system and the monitoring software.


Hardware Sentry - Missing device detection
Missing device detection
Disable missing device detection
By default, Hardware Sentry monitors and detects devices that are missing: i.e., devices that had previously been discovered but may have disappeared during monitoring or after a reboot.
OK
Cancel
Help

When a device is no longer discovered, its *Status* parameter goes into alarm and its label directly shows that it is missing.

The missing device detection feature is enabled by default.

You can however deactivate the feature by right-clicking on the **Hardware icon** > **KM Commands** > **KM Settings > Missing Device Detection**.

Note

Disabling this option when some missing devices have already been detected will trigger a removal of these devices from the monitoring environment.

Monitoring Connectors

By default Hardware Sentry automatically tests which connectors are best-suited to the managed system. Once it decides which connectors are applicable to the managed platform, an instance of the MS_HW_CONNECTORS class is created in the PATROL console and its status is monitored regularly to ensure the availability of the underlying technology.

Example

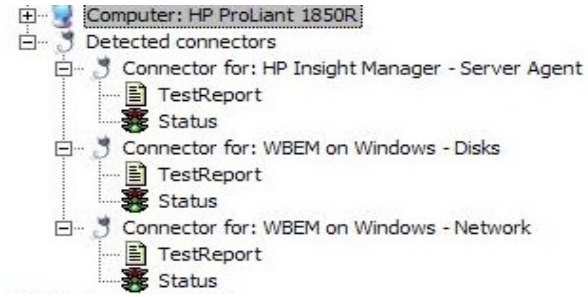
Hardware Sentry is running on an HP Proliant server with HP Insight Management Agent.

Upon startup, Hardware Sentry detects HP Insight Management Agent, and starts using the corresponding connector to discover the server hardware configuration and monitor the discovered devices.

Additionally, Hardware Sentry creates an icon in the PATROL Console representing the HP Insight Management Agent - Server connector.

Every 2 minutes, its *Status* parameter is updated.

If, for some reason, the HP agent stops working, an alarm is raised on the Status parameter and the devices that were discovered through to this connector are taken offline.



The connector monitoring mechanism helps PATROL administrators detect 'real' hardware errors as it enables a higher monitoring accuracy by not confusing errors actually encountered by hardware components with errors owing to a *connector* or *monitoring-tool* failure.

- When connectors are automatically detected by Hardware Sentry, the connectors are grouped under an instance labeled **Detected Connectors.**
- When connectors are manually selected—as for remote monitoring, the connectors are grouped under an instance labeled **Selected Connectors**.

The parameters for connector monitoring are:

Test Report: This parameter describes the tests run to evaluate the availability of the technologies used by this connector to monitor the system.

Status: The parameter displays the status of the connector.

To change the settings of connectors, right-click on the **Hardware icon > KM Commands > This System's Settings > Connection, Credentials and Connectors…**

Thresholds, Alerts & Notification

This section deals with thresholds, alerts and notification. Alert thresholds are dynamically set by Hardware Sentry. However, it is possible change the thresholds, the alert settings as well as the threshold mechanism itself. Hardware Sentry also offers you the possibility of selecting the type of notification (Alert actions) to be sent once an alert is raised. The section has the following sub-sections:

- *Threshold Mechanism Selection*
- *Modifying alert thresholds on parameters*
- *Alert after N times – advanced alert settings*
- *Alert Actions*

Threshold Mechanism Selection

Managing thresholds means selecting/modifying the mechanism by which Hardware Sentry sets thresholds for all parameters of the monitored components. This is done by right-clicking on the **Hardware icon > KM Commands > KM Settings > Threshold Mechanism Selection**

By default, Hardware Sentry automatically sets alert thresholds on the monitored parameters. Depending on the computer it is running on - Hardware Sentry sets different thresholds for the different parameters (temperature, voltage etc.).

The different threshold mechanisms

To set the thresholds, Hardware Sentry uses one of the following two mechanisms, best suited to the managed system:

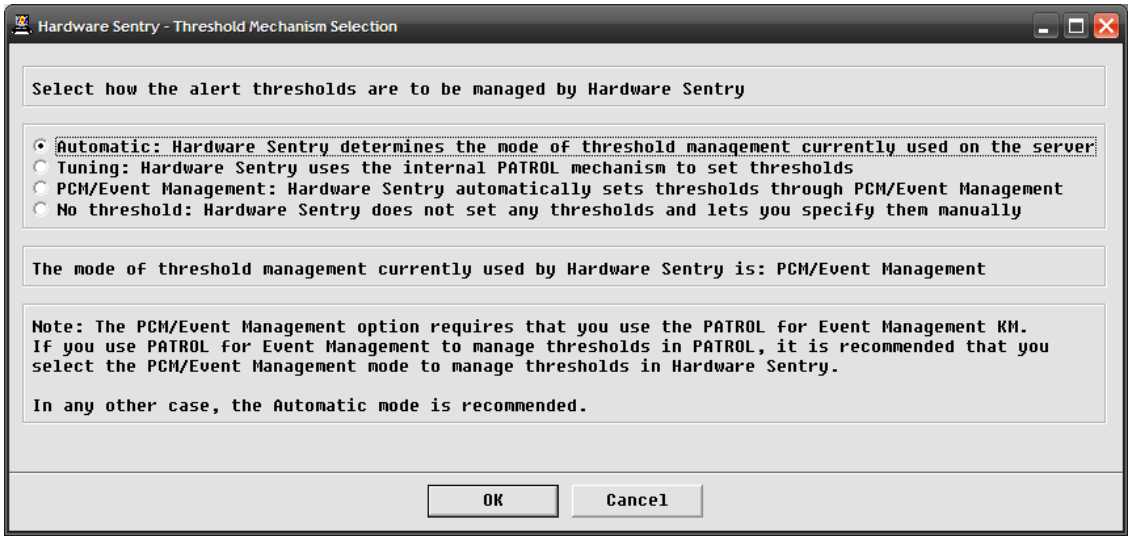
- **Tuning**: A standard internal PATROL mechanism, known as the *Override parameters* in PATROL but called **Tuning** in Hardware Sentry. With this mechanism, Hardware Sentry sets the thresholds of each parameter of each monitored object by setting a specially formatted variable under the /___tuning___ tree in the PATROL Agent configuration.

Or

- **PCM/Event Management: PATROL for Event Management** (formerly known as EventSpring) or **PATROL Configuration Manager** or **PCM**, formerly known as AgentSpring

By default, Hardware Sentry determines which of the above two mechanisms is best suited to the managed system and uses that. This is the **Automatic** setting in the Threshold Mechanism Selection wizard.

To see which mode is currently used for the system, or to modify the **Automatic** mechanism, right-click on: the main **Hardware Sentry/local host icon > KM Commands > KM Settings > Threshold Mechanism Selection...**


Hardware Sentry - Threshold Mechanism Selection
Select how the alert thresholds are to be managed by Hardware Sentry
Automatic: Hardware Sentry determines the mode of threshold management currently used on the server
Tuning: Hardware Sentry uses the internal PATROL mechanism to set thresholds
PCM/Event Management: Hardware Sentry automatically sets thresholds through PCM/Event Management
No threshold: Hardware Sentry does not set any thresholds and lets you specify them manually
The mode of threshold management currently used by Hardware Sentry is: PCM/Event Management
Note: The PCM/Event Management option requires that you use the PATROL for Event Management KM.
If you use PATROL for Event Management to manage thresholds in PATROL, it is recommended that you select the PCM/Event Management mode to manage thresholds in Hardware Sentry.
In any other case, the Automatic mode is recommended.
OK
Cancel

Select one of the following options:

- **Automatic (default):** Hardware Sentry determines and uses the threshold mechanism best suited to the managed system
- **Tuning**: If selected, Hardware Sentry will manage its thresholds through the standard the internal PATROL mechanism (*Override parameters*). Thresholds are stored in the **PATROL Agent configuration** under **the /___tuning___** tree.
- **PCM/Event Management**: if this option is selected, Hardware Sentry will manage its thresholds through the **PCM** or **Event Management** mechanism.

  Thresholds are stored in the **PATROL Agent configuration** under the **/AS** tree. This option requires that you set up the PATROL for Event Management KM on your PATROL Agent. PATROL for Event Management has to be enabled and preloaded.

  Note

  If you use PATROL for Event Management to manage thresholds in PATROL, it is strongly recommended that you use this option in Hardware Sentry too.

  Warning!

  In order to avoid side effects and unpredictable behavior, if you select the "PCM/Event Management" thresholds management option, Hardware Sentry will automatically remove the thresholds set through the other method. That is: if you select the "PCM/Event Management" option, Hardware Sentry will automatically remove all the thresholds stored in the /___tuning___ tree in the PATROL Agent configuration.

- **No Thresholds**: Hardware Sentry will not set any thresholds on the monitored objects. You are required to set them manually.

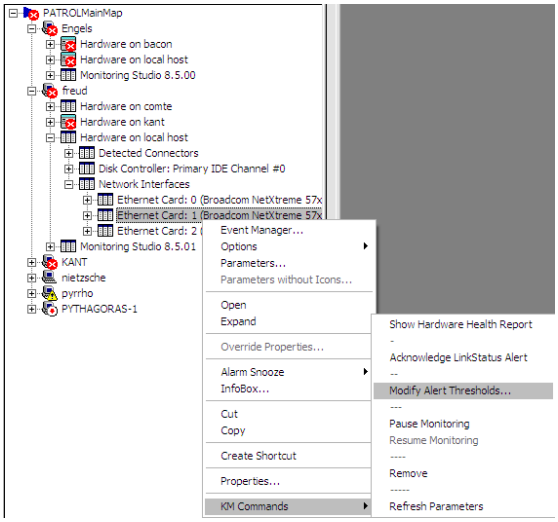
For details on how to manually set thresholds on the parameters, please see the next topic: *Modifying alert thresholds*.

Modifying alert thresholds on parameters

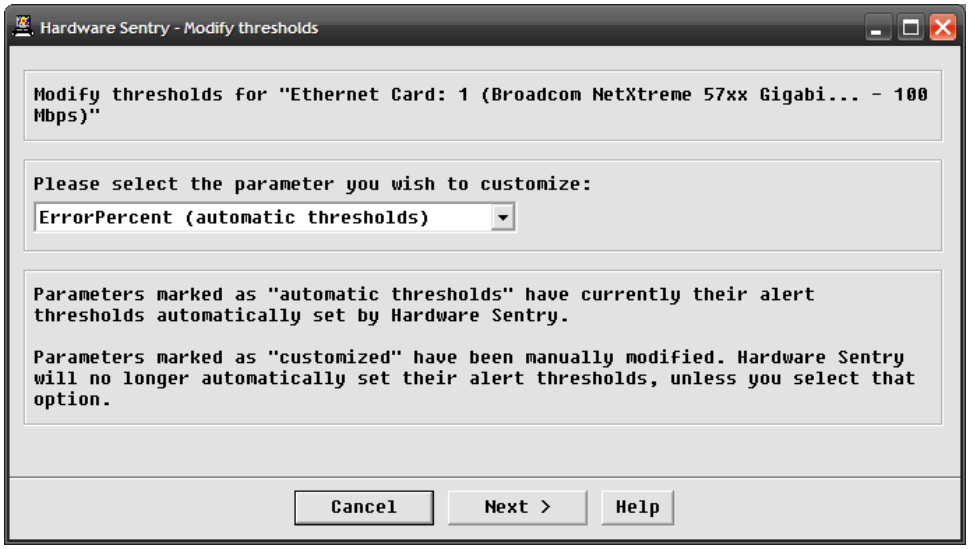
Whenever possible, Hardware Sentry automatically sets thresholds for parameters. These thresholds are retrieved from the information available from the hardware agents and they are generally accurate.

Generally, there is no need to modify these thresholds but in case Hardware Sentry cannot obtain them, or if you prefer a more fault-tolerant monitoring, you can modify the thresholds of each parameter through the command menu.

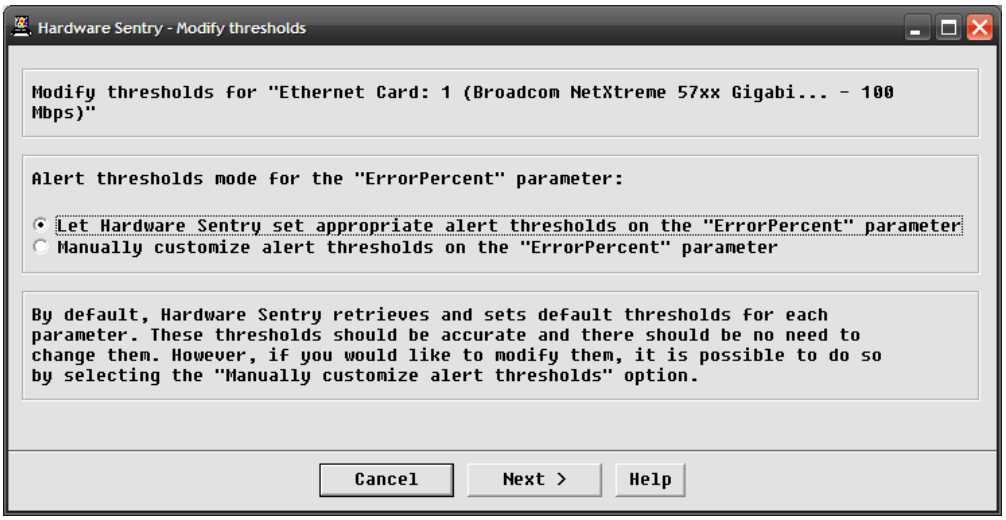
1. Right-click on the **monitored sensor/device** (not directly on the parameter) **> KM Commands > Modify Alert Thresholds**.



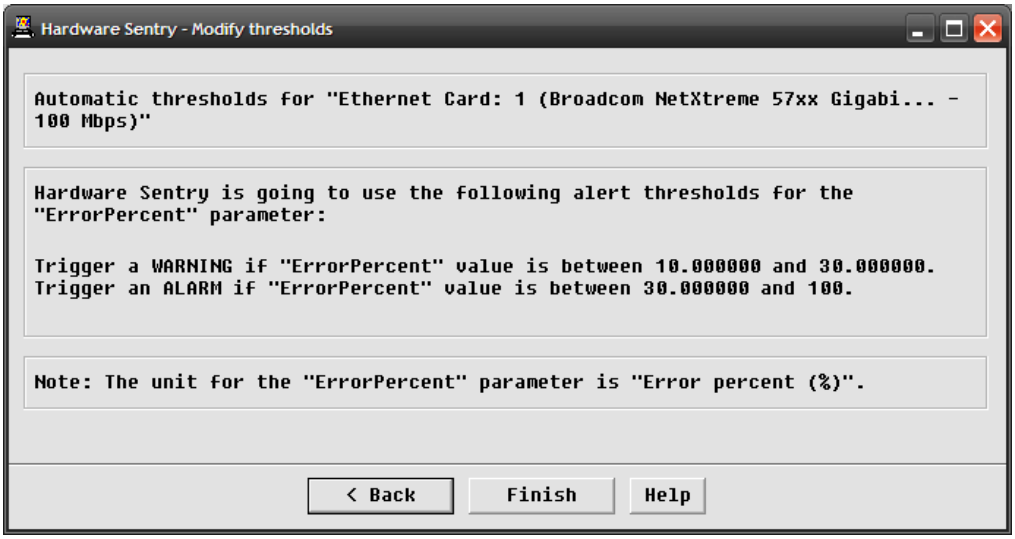
2. The first panel shows the list of parameters for that particular object, select the parameter whose thresholds you wish to modify:


Hardware Sentry - Modify thresholds
Modify thresholds for "Ethernet Card: 1 (Broadcom NetXtreme 57xx Gigabi... - 100 Mbps)"
Please select the parameter you wish to customize:
ErrorPercent (automatic thresholds)
Parameters marked as "automatic thresholds" have currently their alert thresholds automatically set by Hardware Sentry.
Parameters marked as "customized" have been manually modified. Hardware Sentry will no longer automatically set their alert thresholds, unless you select that option.
Cancel
Next >
Help

3. Select the mode:

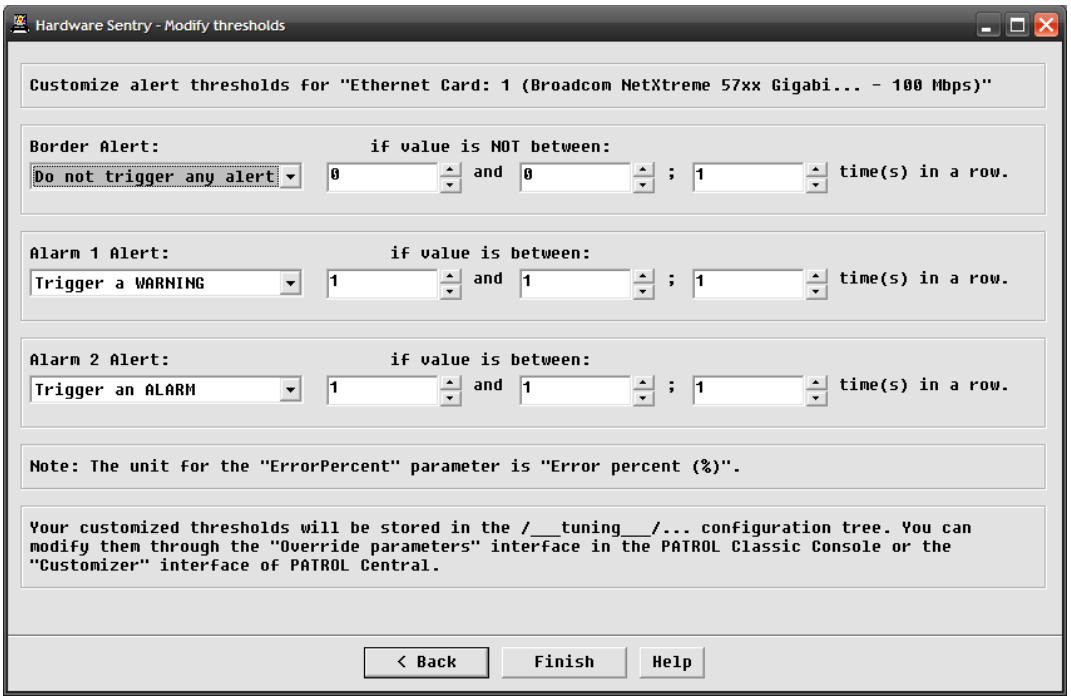

Hardware Sentry - Modify thresholds
Modify thresholds for "Ethernet Card: 1 (Broadcom NetXtreme 57xx Gigabi... - 100 Mbps)"
Alert thresholds mode for the "ErrorPercent" parameter:
Let Hardware Sentry set appropriate alert thresholds on the "ErrorPercent" parameter
Manually customize alert thresholds on the "ErrorPercent" parameter
By default, Hardware Sentry retrieves and sets default thresholds for each parameter. These thresholds should be accurate and there should be no need to change them. However, if you would like to modify them, it is possible to do so by selecting the "Manually customize alert thresholds" option.
Cancel
Next >
Help

- **Let Hardware Sentry set appropriate alert thresholds**: Select this option (**recommended**) to let Hardware Sentry determine and set the alert thresholds best suited to the parameter/device/system. **Next** brings to the following panel that displays the threshold values:


Hardware Sentry - Modify thresholds
Automatic thresholds for "Ethernet Card: 1 (Broadcom NetXtreme 57xx Gigabi... - 100 Mbps)"
Hardware Sentry is going to use the following alert thresholds for the "ErrorPercent" parameter:
Trigger a WARNING if "ErrorPercent" value is between 10.000000 and 30.000000.
Trigger an ALARM if "ErrorPercent" value is between 30.000000 and 100.
Note: The unit for the "ErrorPercent" parameter is "Error percent (%)".
< Back
Finish
Help

Confirm the selection by clicking **Finish** or click **Back** to manually set thresholds for the parameter.

- **Manually customize alert thresholds**: Selecting this option brings you to a panel where you are can set new thresholds for the parameter.



Automatic Threshold Mechanism Setting

If you select the **Automatic** thresholds mechanism option (see *Threshold Mechanism Selection*), your customized thresholds are stored under the /___tuning___ tree in the PATROL Agent configuration and then can be modified through the “Override parameter" feature of the PATROL Console.

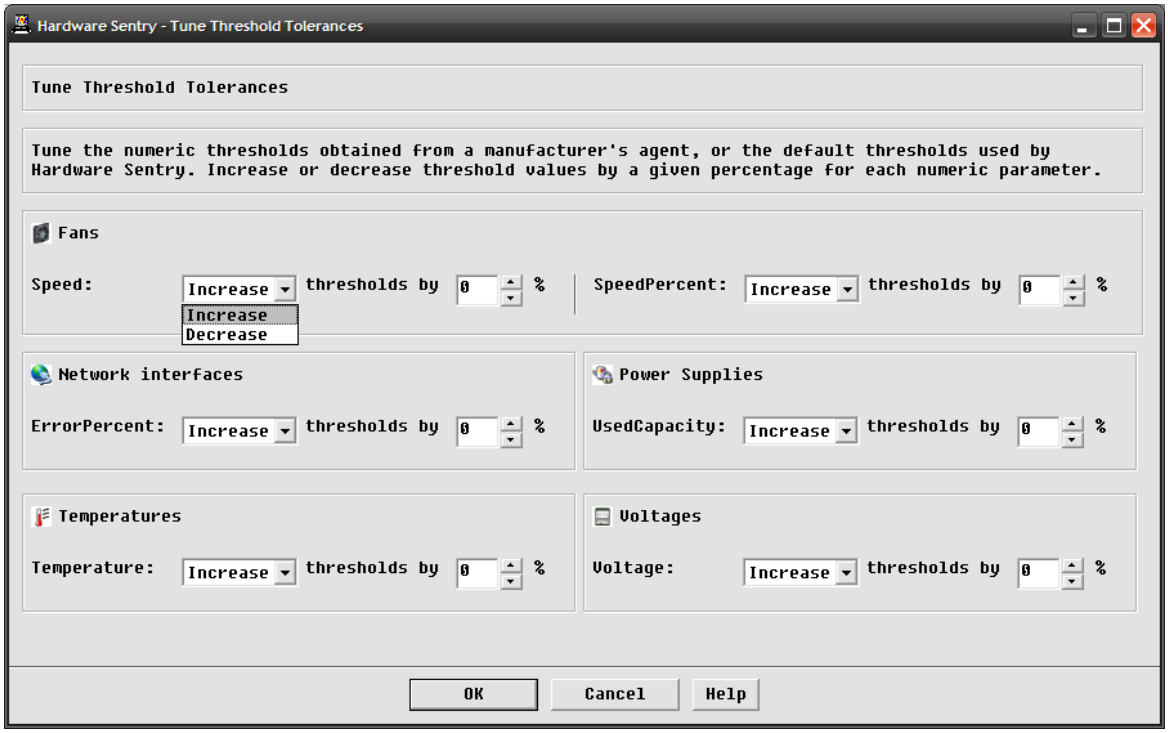
PCM/Event Management Threshold Mechanism Setting

If you select the **PCM/Event Management** thresholds management option, your customized thresholds are stored under the /AS tree in the PATROL Agent configuration and then can be modified through the PATROL for Event Management (EventSpring) interface or through the PATROL Configuration Manager graphical user interface.

Tune Threshold Tolerance

The Tune Threshold Tolerance feature enables you to fine-tune your monitoring thresholds for those parameters that have numeric values. This feature can be helpful to either tighten your monitoring or make it more flexible to prevent frequent alerts. The fine-tuning would depend on each system's behavior and your specific needs.

To access this feature, right-click on **the Hardware icon > KM Commands > This System's Settings > Tune Threshold Tolerance**.



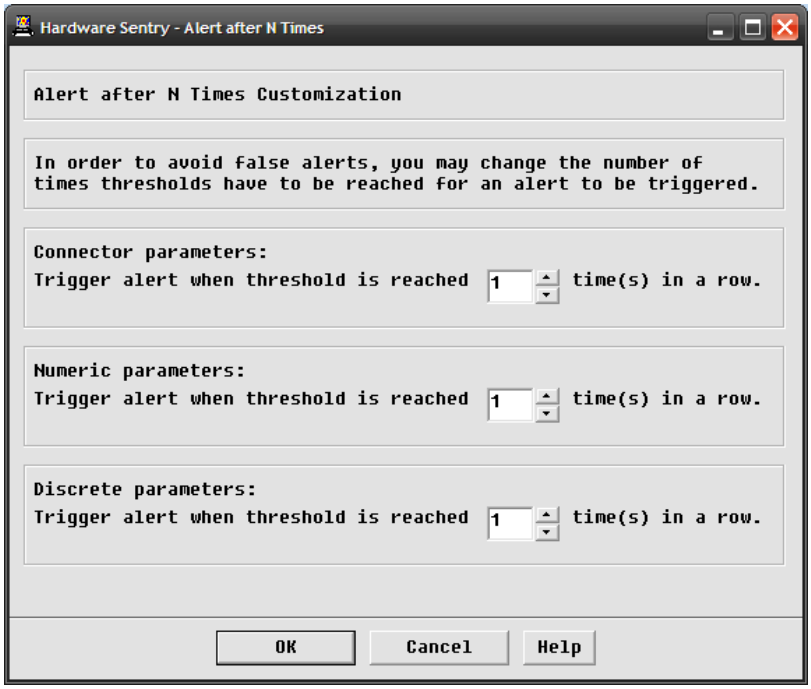
Threshold tolerance can be fine-tuned by increasing or decreasing the values in percentages for numeric parameters of the following components:

- **Fan**: *Speed* and *SpeedPercent*
- **Network interface**: *ErrorPercent*
- **Temperature**: *Temperature*
- **Power supplies**: *UsedCapacity*
- **Voltages**: *Voltage*

Alert after *N* times – advanced alert settings

Hardware Sentry offers a global advanced alert setting in order to prevent false alerts. You can now set/modify the number of times thresholds can be breached *before* triggering an alert.

This advanced alert setting, commonly known as "Alert after N times" is accessible by right-clicking the main **Hardware icon > This System's Settings** > **Alert after N Times…**


Hardware Sentry - Alert after N Times
Alert after N Times Customization
In order to avoid false alerts, you may change the number of times thresholds have to be reached for an alert to be triggered.
Connector parameters:
Trigger alert when threshold is reached 1 time(s) in a row.
Numeric parameters:
Trigger alert when threshold is reached 1 time(s) in a row.
Discrete parameters:
Trigger alert when threshold is reached 1 time(s) in a row.
OK
Cancel
Help

Hardware Sentry parameters can be categorized in three main groups:

- **Connector parameters**: Status parameters of the MS_HW_CONNECTORS class
- **Numeric parameters**: Parameters that have numeric values such as *Temperature, Voltage, ErrorPercent*, etc.
- **Discrete parameters**: Parameters that have values such as 0=OK, 1=Degraded/Predicted Failure, 2 = Failed etc. These parameters display the status of the device. Example: *Status, LinkStatus, PredictedFailure, ControllerStatus* etc.

By setting or changing the number of times a threshold can be breached *before* it triggers an alert – you can avoid unnecessary false alerts.

This is a "global" setting, and applies to the parameters of all the monitored devices of the system.

Alert Actions

Alert Actions enables the PATROL administrator to choose specific actions to be performed when a hardware error or failure is detected. With the Alert Actions feature, it is possible to either:

- Customize the way a hardware problem notification is performed, or
- Specify a recovery action to be run when a problem occurs

Hardware Sentry can be configured to run one, several, or all types of Alert Actions when an alert is triggered regarding the monitored hardware.

By default, upon hardware failure, Hardware Sentry triggers a PATROL event and annotates the parameter's graph with a comprehensive report of the problem, giving details about the failure, the possible consequences and the recommended action to solve the problem.

The Alert Actions that can be performed by Hardware Sentry are:

- *Trigger a PATROL Event*
- *Annotate the Parameter's Graph*
- *Execute an OS command*
- *Execute a PSL command*
- *Send a Pop-up to the PATROL Consoles*
- *Write a line to a LOG file*
- *Send a Basic SNMP trap*
- *Send a custom SNMP trap (advanced)*

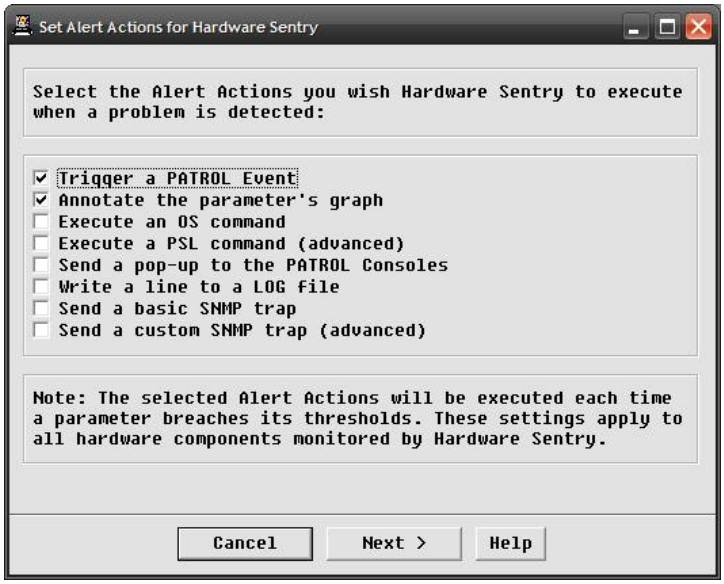
Alert Actions are highly customizable. One can customize the string that is sent through SNMP, set the username/password that is used to execute the OS Command, define the content of the PATROL event sent by Hardware Sentry, etc.

Additional information regarding the alert, such as the parameter name or its value, can be available by using *Alert Action Macro Variables*. This information can be used to further customize the Alert Action triggered by Hardware Sentry and provide more details about the problem that occurs.

Editing Alert Actions

To modify the Alert Actions executed by Hardware Sentry upon a hardware failure, right-click on the main **Hardware Sentry/local host icon > KM Commands > KM Settings > Edit Alert Actions…**

Select the Alert Actions to be executed

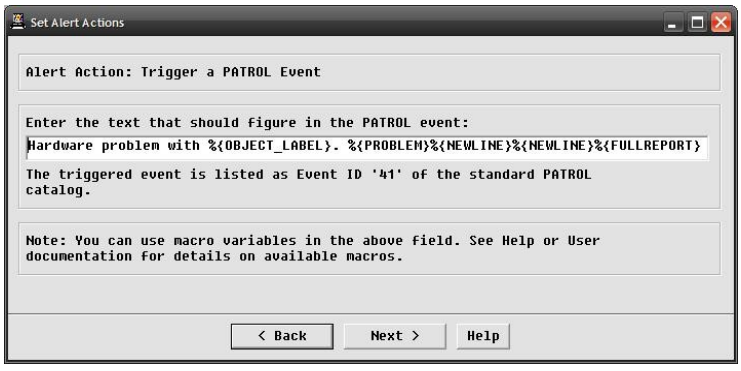

Set Alert Actions for Hardware Sentry
Select the Alert Actions you wish Hardware Sentry to execute when a problem is detected:
Trigger a PATROL Event
Annotate the parameter's graph
Execute an OS command
Execute a PSL command (advanced)
Send a pop-up to the PATROL Consoles
Write a line to a LOG file
Send a basic SNMP trap
Send a custom SNMP trap (advanced)
Note: The selected Alert Actions will be executed each time a parameter breaches its thresholds. These settings apply to all hardware components monitored by Hardware Sentry.
Cancel
Next >
Help

Check the boxes corresponding to the actions you would like executed upon a hardware failure.

By default, Hardware Sentry:

- Triggers a PATROL event
- Annotates the parameter that raises the alert.

Trigger a PATROL Event


Set Alert Actions
Alert Action: Trigger a PATROL Event
Enter the text that should figure in the PATROL event:
Hardware problem with %{OBJECT_LABEL}. %{PROBLEM}%{NEWLINE}%{NEWLINE}%{FULLREPORT}
The triggered event is listed as Event ID '41' of the standard PATROL catalog.
Note: You can use macro variables in the above field. See Help or User documentation for details on available macros.
< Back
Next >
Help

If you select **Trigger a PATROL Event**, you need to enter the string that will be displayed with the event. A PATROL Event can be viewed from:

- Standard PATROL Consoles (Classic Console, PATROL Central)
- PATROL Enterprise Manager
- BMC Impact Manager
- Other third-party products that interface with PATROL.

Note

As this action is triggered by default by Hardware Sentry, there is no need to "enter" the text in the field unless you wish to modify the content that it reports in PATROL events.

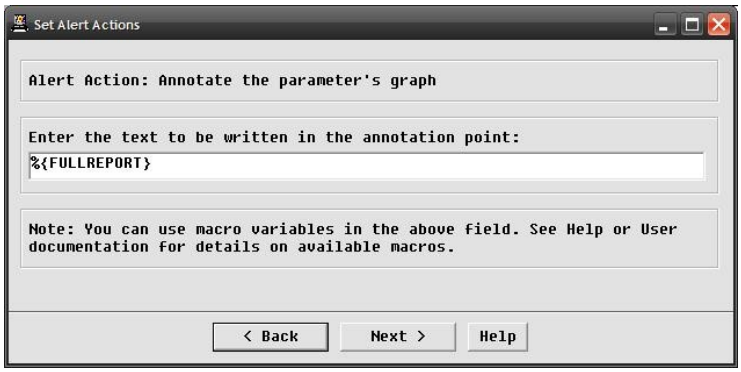
Note

The PATROL event that is triggered is the '41' event from the standard PATROL catalog.

Note

You can use macros that will be replaced at runtime. The list of available macros is described under the section *Alert Action Macro Variables*.

Annotate the Parameter's Graph

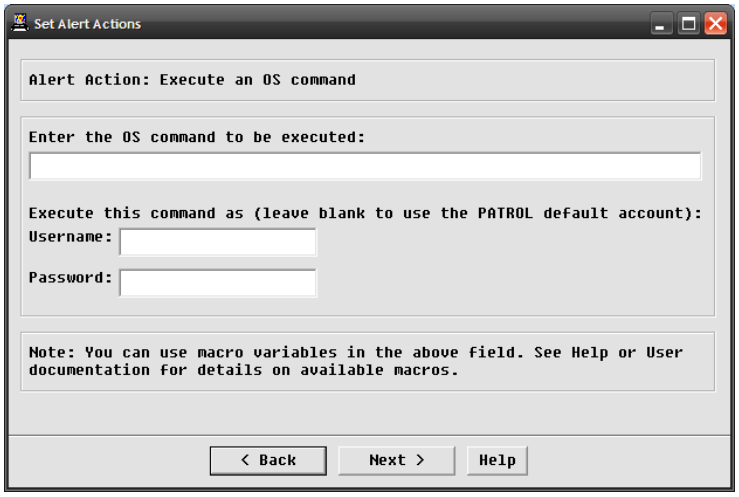

Set Alert Actions
Alert Action: Annotate the parameter's graph
Enter the text to be written in the annotation point:
%{FULLREPORT}
Note: You can use macro variables in the above field. See Help or User documentation for details on available macros.
< Back
Next >
Help

If you select the **Annotate the parameter's graph** action, you need to enter the string that will be displayed within the annotation point.

Note

You can use macros that will be replaced at runtime. The list of available macros is described in *Alert Action Macro Variables*.

Execute an OS command


Set Alert Actions
Alert Action: Execute an OS command
Enter the OS command to be executed:
Execute this command as (leave blank to use the PATROL default account):
Username:
Password:
Note: You can use macro variables in the above field. See Help or User documentation for details on available macros.
< Back
Next >
Help

If you select the **Execute an OS command** action, you need to:

- Enter a command line to be executed
- Enter a user and password used to run the command.

The command can be a program utility or a script shell, and can have arguments.

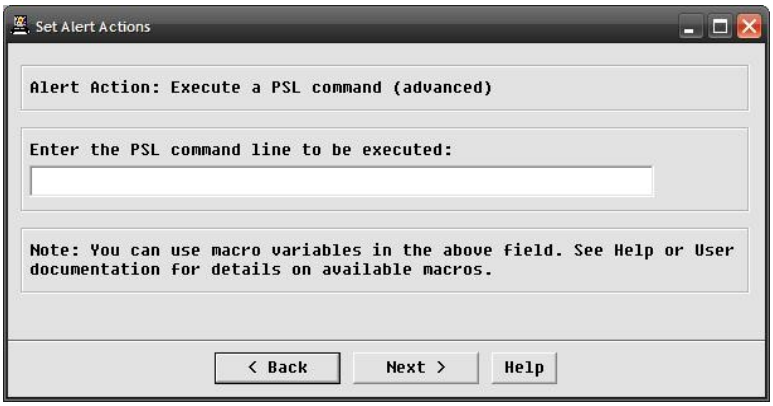
Warning!

The command must be non-interactive (no window, no user input).

Note

You can use macros that will be replaced at runtime. The list of available macros is described in the section *Alert Action Macro Variables*.

Execute a PSL command


Set Alert Actions
Alert Action: Execute a PSL command (advanced)
Enter the PSL command line to be executed:
Note: You can use macro variables in the above field. See Help or User documentation for details on available macros.
< Back
Next >
Help

If you select the **Execute a PSL command** action, you need to enter the PSL statement to be executed by the PATROL Agent. Although, only a single line is permitted, it can have several PSL instructions.

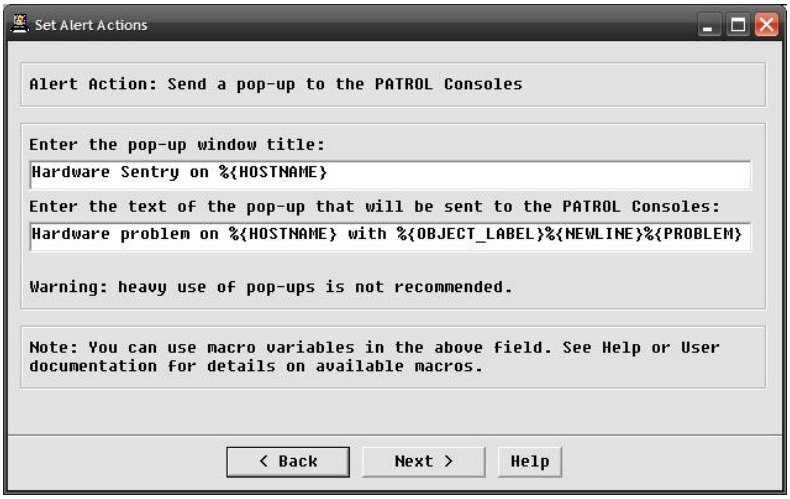
Warning!

The PSL command is recommended for PATROL advanced users only.

Note

You can use macros that will be replaced at runtime. The list of available macros is described in the section *Alert Action Macro Variables*.

Send a Pop-up to the PATROL Consoles


Set Alert Actions
Alert Action: Send a pop-up to the PATROL Consoles
Enter the pop-up window title:
Hardware Sentry on %{HOSTNAME}
Enter the text of the pop-up that will be sent to the PATROL Consoles:
Hardware problem on %{HOSTNAME} with %{OBJECT_LABEL}%{NEWLINE}%{PROBLEM}
Warning: heavy use of pop-ups is not recommended.
Note: You can use macro variables in the above field. See Help or User documentation for details on available macros.
< Back
Next >
Help

If you select the **Send a pop-up to the PATROL Consoles** action, you need to enter the message that will be displayed in the pop-up as well as the title of the pop-up window.

Warning!

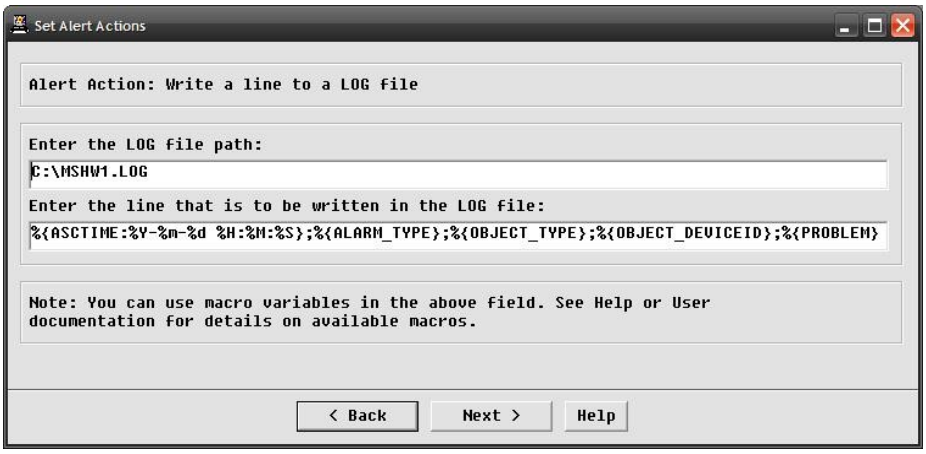
Too many pop-ups could annoy the operators.

Note

You can use macros that will be replaced at runtime. The list of available macros is described in the section *Alert Action Macro Variables*.

Write a line to a LOG file

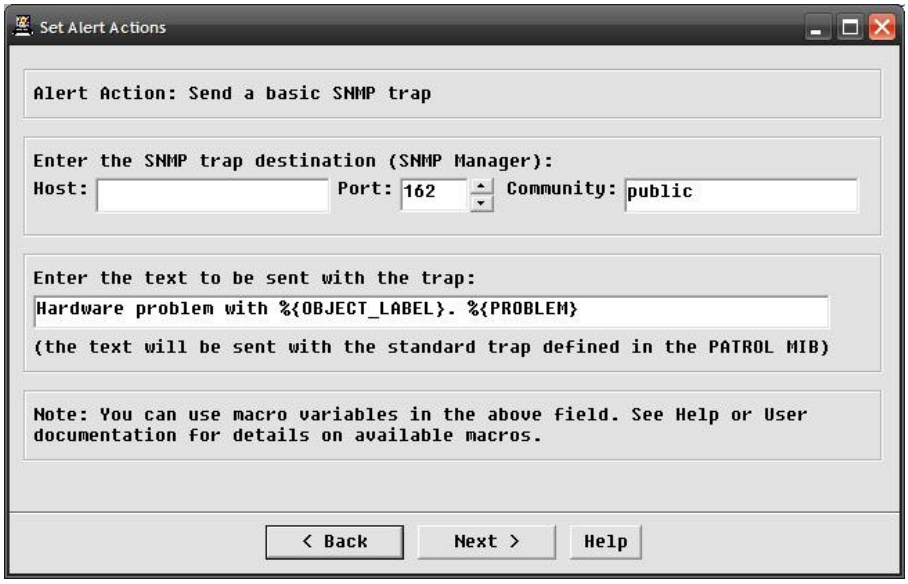
If you select the **Write a line to a LOG file** action, you need to enter the LOG file path where Hardware Sentry will write a line, as well as the content of the line to be written.


Set Alert Actions
Alert Action: Write a line to a LOG file
Enter the LOG file path:
C:\MSHW1.LOG
Enter the line that is to be written in the LOG file:
%{ASCTIME:%Y-%m-%d %H:%M:%S};%{ALARM_TYPE};%{OBJECT_TYPE};%{OBJECT_DEVICEID};%{PROBLEM}
Note: You can use macro variables in the above field. See Help or User documentation for details on available macros.
< Back
Next >
Help

Note

You can use macros that will be replaced at runtime. The list of available macros is described later in this chapter.

Send a Basic SNMP trap


Set Alert Actions
Alert Action: Send a basic SNMP trap
Enter the SNMP trap destination (SNMP Manager):
Host:
Port: 162
Community: public
Enter the text to be sent with the trap:
Hardware problem with %{OBJECT_LABEL}. %{PROBLEM}
(the text will be sent with the standard trap defined in the PATROL MIB)
Note: You can use macro variables in the above field. See Help or User documentation for details on available macros.
< Back
Next >
Help

If you select the **Send a basic SNMP trap action**, you need to enter:

The IP address or hostname of the SNMP manager that the trap will be issued to

The SNMP community string used by the SNMP manager.

The text that will be sent in the SNMP trap.

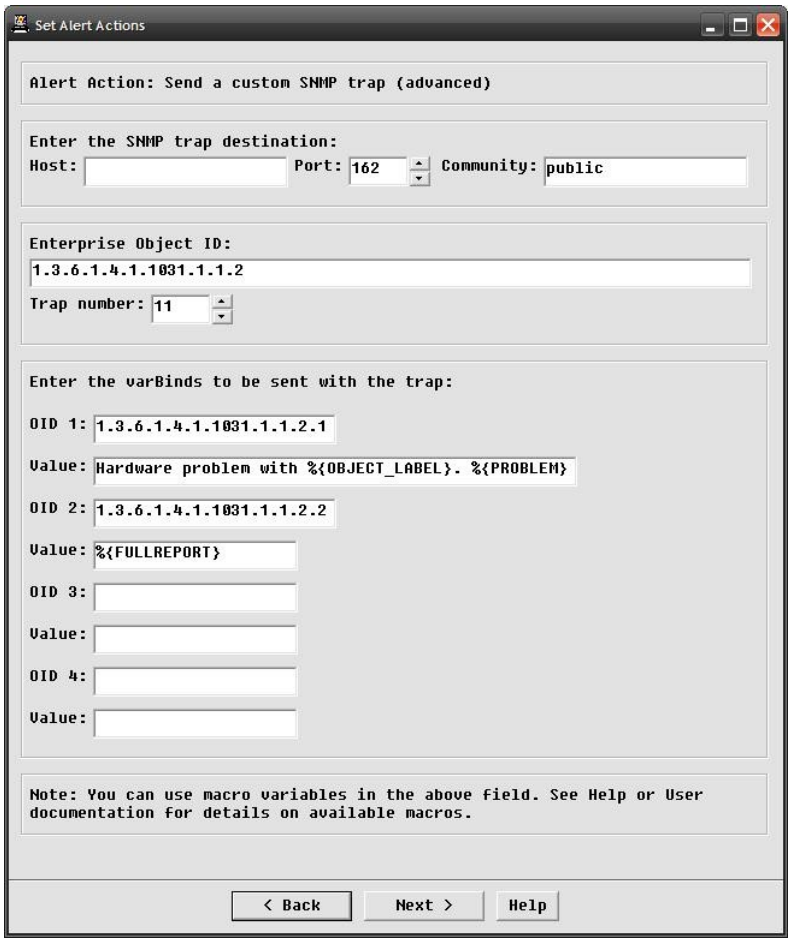
Note

Upon a hardware failure, Hardware Sentry will send the trap that is defined in the PATROL MIB (Trap number 11, Enterprise ID: 1.3.6.1.4.1.1031.1.1.2, the text is stored in the 1.3.6.1.4.1.1031.1.1.2.1 OID).

Note

You can use macros that will be replaced at runtime. The list of available macros is given in the section *Alert Action Macro Variables*.

Send a custom SNMP trap (advanced)



If you select the **Send a custom SNMP trap** action, you need to enter the following:

- The IP address or hostname of the SNMP manager that the trap will be issued to
- The SNMP community string used by the SNMP manager
- All the characteristics of the trap: Enterprise ID, trap specific number and up to 4 varbinds

Note

You can use macros that will be replaced at runtime. The list of available macros is described later in this chapter.

Alert Action Macro Variables

Macro variables can be used in the Alert Actions to customize a string with information related to the encountered hardware failure (display name of the faulty object, value of the parameter, description of the problem, etc.)

Example

You can configure Hardware Sentry to trigger a PATROL event containing the display name of the faulty object by entering something like *Hardware problem with %{ OBJECT_NAME}* in the Trigger a PATROL Event dialog box.

Note

You can use several macros at one time.

The table below recapitulates macros available for Alert Actions.

Macro	Description
%{PARAMETER_NAME}	Name of the parameter that triggered the alert Example: *PredictedFailure*
%{VALUE}	Formatted value (with unit) of the parameter that triggered the alert Example: 67.3 °C
%{RAW_VALUE}	Raw value of the parameter that triggered the alert Example: 67.30000
%{ALARM_TYPE}	Alarm type (INFORMATION, WARNING or ALARM) Example: ALARM
%{PROBLEM}	Description of the problem encountered by the monitored device Example: The speed of this fan is critically low (1503 rpm)
%{CONSEQUENCE}	Description of the possible consequence of the detected problem Example: The temperature of the chip, component or device that was cooled by this fan should grow quickly. This can lead to severe hardware damage and system crashes
%{RECOMMENDED_ACTION}	Recommended action to solve the problem Example: Quickly check if the fan is really no more cooling the system. If so, replace the fan.

Macro	Description
%{OBJECT_ID}	PATROL internal ID of the instance that triggered the alert Example: MS_HW_DellOpenManagehdf_11
%{OBJECT_LABEL}	Display name of the instance that triggered the alert Example: Fan: 1.1 (CPU 1)
%{OBJECT_CLASS}	Class of the instance that triggered the alert Example: MS_HW_FAN
%{OBJECT_TYPE}	Type of the device that triggered the alert Example: Fan
%{OBJECT_DEVICEID}	Hardware Sentry internal device ID of the instance that triggered the alert Example: 1.1
%{PARENT_ID}	PATROL internal ID of the object that the faulty instance is attached to Example: MS_HW_DellOpenManagehdf_1
%{PARENT_LABEL}	Display name of the object that the faulty instance is attached to Example: Computer: Dell PowerEdge 1600SC
%{PARENT_CLASS}	Class of the object that the faulty instance is attached to Example: MS_HW_ENCLOSURE
%{PARENT_TYPE}	Type of the object that the faulty instance is attached to Example: Computer enclosure
%{PARENT_DEVICEID}	Hardware Sentry internal device ID of the object that the faulty instance is attached to Example: 1
%{HOSTNAME}	Host name of the computer that the PATROL Agent is running on Example: SENTRYTEST003
%{DATE}	Current date in the YYYY-MM-dd format Example: 2005-6-23
%{TIME}	Current time in the HH:MM:SS format Example: 11:14:53

Macro	Description
%{ASCTIME:…}	Current date and time formatted as specified in the macro Example: %{ASCTIME:%m %d %T %Y} will produce Jun 6 11:14:53 2005 The available formats for the %{ ASCTIME :…} macro are listed in the asctime() description of the PSL Reference Guide (Book 2).
%{/variable_name}	Value of the *variable_name* instance variable Example: %{/worstParam} will give the name of the "worst parameter" of the instance that triggered the alert. This feature is recommended for advanced users only!
%{NEWLINE} **%{\n}**	Linefeed This is useful to produce multi-line information.
%{FULLREPORT}	Full hardware health report about the instance that triggered the alert Example: See the output of the "Instant Hardware Health Report" Menu command

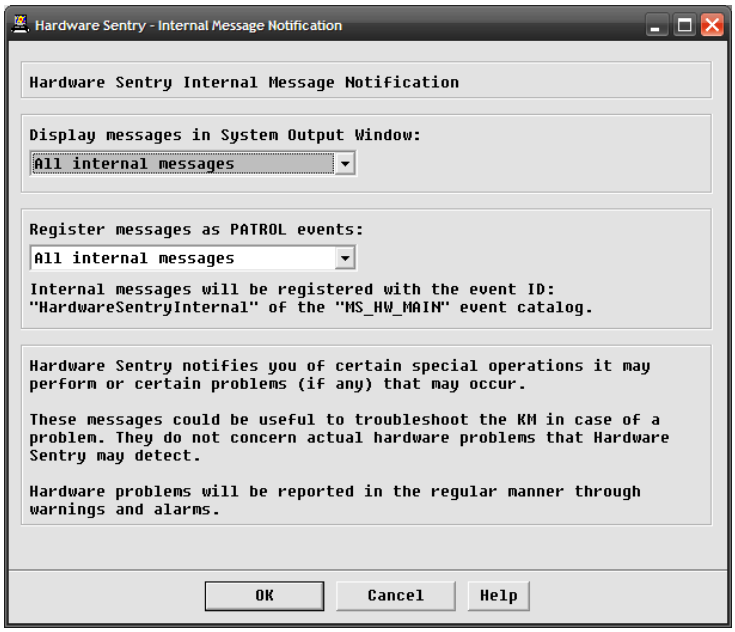
Internal KM Issues Notification

Internal KM Issues Notification was previously known as the KM command *Internal Message Notification* and prior to that as *Show/Hide Information Messages.*

This notification feature enables Hardware Sentry to inform you of any internal problems that may occur or any special operations it may perform. The objective of this notification is to help resolve an issue (if any), *other than* hardware problems – which are reported through the regular system of warnings and alerts. This feature is useful to find out more about any anomalies that may occur.

By right clicking on **Hardware icon > KM Commands > Internal KM issues Notification**, you can set the kind of messages you would like to be notified about:

- All internal messages
- Only internal problems
- No internal message


Hardware Sentry - Internal Message Notification
Hardware Sentry Internal Message Notification
Display messages in System Output Window:
All internal messages
Register messages as PATROL events:
All internal messages
Internal messages will be registered with the event ID:
"HardwareSentryInternal" of the "MS_HW_MAIN" event catalog.
Hardware Sentry notifies you of certain special operations it may perform or certain problems (if any) that may occur.
These messages could be useful to troubleshoot the KM in case of a problem. They do not concern actual hardware problems that Hardware Sentry may detect.
Hardware problems will be reported in the regular manner through warnings and alarms.
OK
Cancel
Help

By default, all internal messages are sent to the System Output Window and are also registered as PATROL events (event ID “HardwareSentryInternal” of the MS_HW_MAIN event catalog).

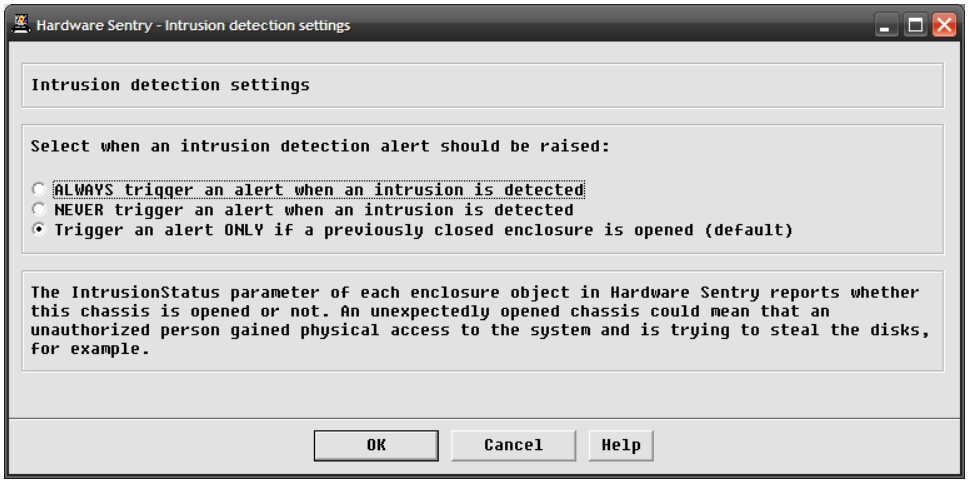
Note

Internal errors are registered as events type “ERROR” (they appear in orange in PATROL Event Manager). Internal warnings are registered as “WARNING” and Informational messages are registered as “INFORMATION”.

Intrusion Detection Alerts

Hardware Sentry triggers alerts if the enclosure/chassis of your managed system has been opened. An unexpectedly opened chassis could imply that the system is physically accessed by an unauthorized person.

The Intrusion Detection Alert feature enables you to select the alert conditions. Right-click on the **Hardware icon > KM Commands > KM Settings > Intrusion Detection Alerts**:

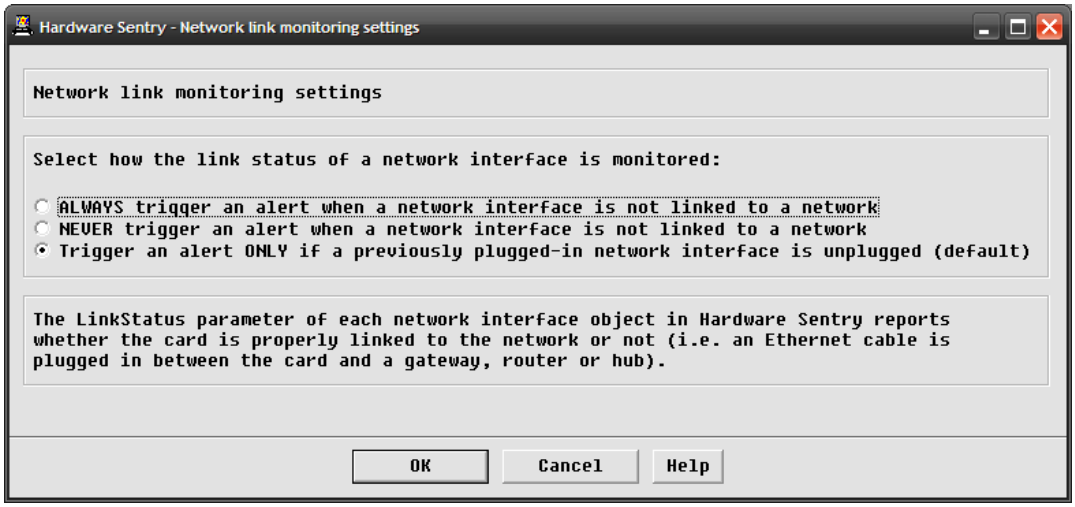

Hardware Sentry - Intrusion detection settings
Intrusion detection settings
Select when an intrusion detection alert should be raised:
ALWAYS trigger an alert when an intrusion is detected
NEVER trigger an alert when an intrusion is detected
Trigger an alert ONLY if a previously closed enclosure is opened (default)
The IntrusionStatus parameter of each enclosure object in Hardware Sentry reports whether this chassis is opened or not. An unexpectedly opened chassis could mean that an unauthorized person gained physical access to the system and is trying to steal the disks, for example.
OK
Cancel
Help

By default, Hardware Sentry triggers an alert ONLY if a previously closed enclosure is opened.

Network Link Alerts

Hardware Sentry triggers alerts if it detects a break in the network link. By default, this alert is raised ONLY if a previously detected network link is broken.

To change the default setting and select when these alerts should be raised, right-click on the on the **Hardware icon > KM Commands > KM Settings > Network Link Alerts**:

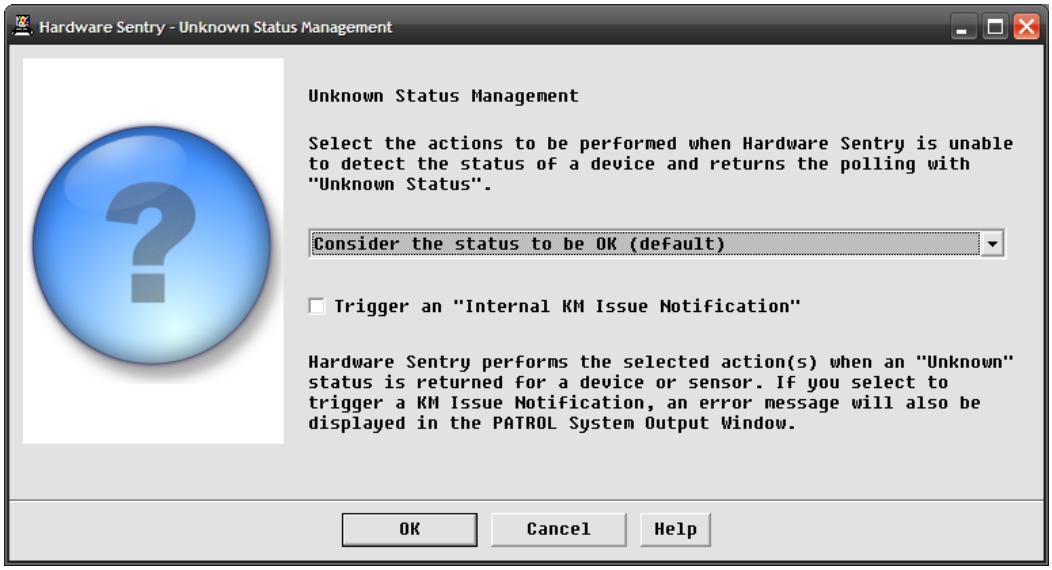

Hardware Sentry - Network link monitoring settings
Network link monitoring settings
Select how the link status of a network interface is monitored:
ALWAYS trigger an alert when a network interface is not linked to a network
NEVER trigger an alert when a network interface is not linked to a network
Trigger an alert ONLY if a previously plugged-in network interface is unplugged (default)
The LinkStatus parameter of each network interface object in Hardware Sentry reports whether the card is properly linked to the network or not (i.e. an Ethernet cable is plugged in between the card and a gateway, router or hub).
OK
Cancel
Help

Unknown Status Management

At times, although rare, Hardware Sentry is unable to detect the status of a monitored device, and it returns the poll with "Unknown Status". If this occurs, you can configure Hardware Sentry to perform certain actions:

- Consider the status to be OK (default)
- Ignore status and do not feed parameter
- Trigger a warning on the Status parameter
- Trigger an alarm on the Status parameter

To access this feature, right-click on the **Hardware icon > KM Commands > KM Settings > Unknown Status Management**:


Hardware Sentry - Unknown Status Management
Unknown Status Management
Select the actions to be performed when Hardware Sentry is unable to detect the status of a device and returns the polling with "Unknown Status".
Consider the status to be OK (default)
Trigger an "Internal KM Issue Notification"
Hardware Sentry performs the selected action(s) when an "Unknown" status is returned for a device or sensor. If you select to trigger a KM Issue Notification, an error message will also be displayed in the PATROL System Output Window.
OK
Cancel
Help

Configuration and Administrative Tasks

This section deals with information on basic configuration and administrative tasks such as:

- *Set connection, credentials and connectors on the local host*
- *Customize the discovery cycle*
- *Customize the polling interval*
- *Enter a license key for Hardware Sentry*
- *Distribute the license over several computers*
- *Pause the monitoring of an object*
- *Reinitialize the KM*
- *Restore the monitoring of a device after removal*
- *Show an instant Hardware Health report*
- *Schedule Hardware Health reports*
- *Terminate the monitoring of a device*
- *Trigger a KM discovery*
- *Display labels in the UNIX Console mode*

Note

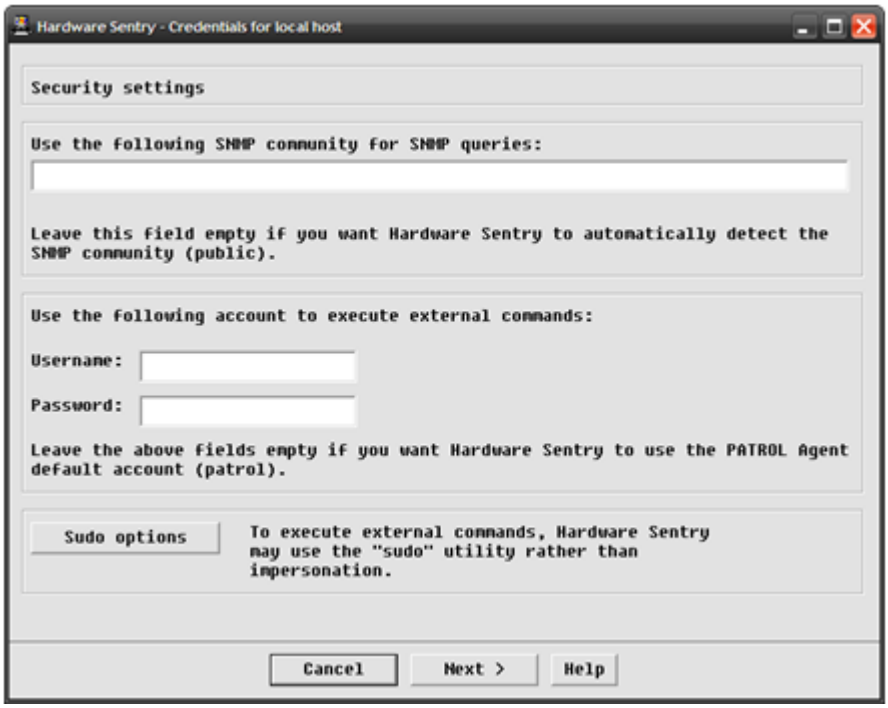
The Reference Guide has a section on *Configuration Variables* which contains list of global and host-specific configuration variables as well as "time" macros. This information is also available in an online format in the Hardware Sentry Online Technical Library, as well as in the online help of the KM.

Set connection, credentials and connectors on the local host

In order to access security settings and connector selection features, right-click the local host's **Hardware icon > KM Commands > This System's Settings > Connection, Credentials and Connectors**.

This wizard begins with security settings and is then followed by the connector selection step.

Security settings


Hardware Sentry - Credentials for local host
Security settings
Use the following SNMP community for SNMP queries:
Leave this field empty if you want Hardware Sentry to automatically detect the SNMP community (public).
Use the following account to execute external commands:
Username:
Password:
Leave the above fields empty if you want Hardware Sentry to use the PATROL Agent default account (patrol).
Sudo options
To execute external commands, Hardware Sentry may use the "sudo" utility rather than impersonation.
Cancel
Next >
Help

SNMP Community

Hardware Sentry allows you to set or modify the SNMP community that will be used for SNMP queries.

Enter the custom SNMP community string in the first field or leave this field blank if you want Hardware Sentry to automatically detect the SNMP community (public).

Using an alternate SNMP community can be required in secured network environments where all the SNMP agents are configured in a customized community.

Alternate user account

Enter the user credentials of the alternate account to execute external commands, or leave blank to consider default PATROL account.

Using an alternate account, i.e. an account different from the default PATROL account to execute external commands (OS commands and WBEM queries) is required in some secured systems where the default PATROL account does not have all the privileges required in order to perform queries on certain hardware devices.

This is also true for HP-UX systems (for physical disks) as well as IBM xSeries computers under Linux (for WBEM requests). Please refer to the platform-specific guides for specific details.

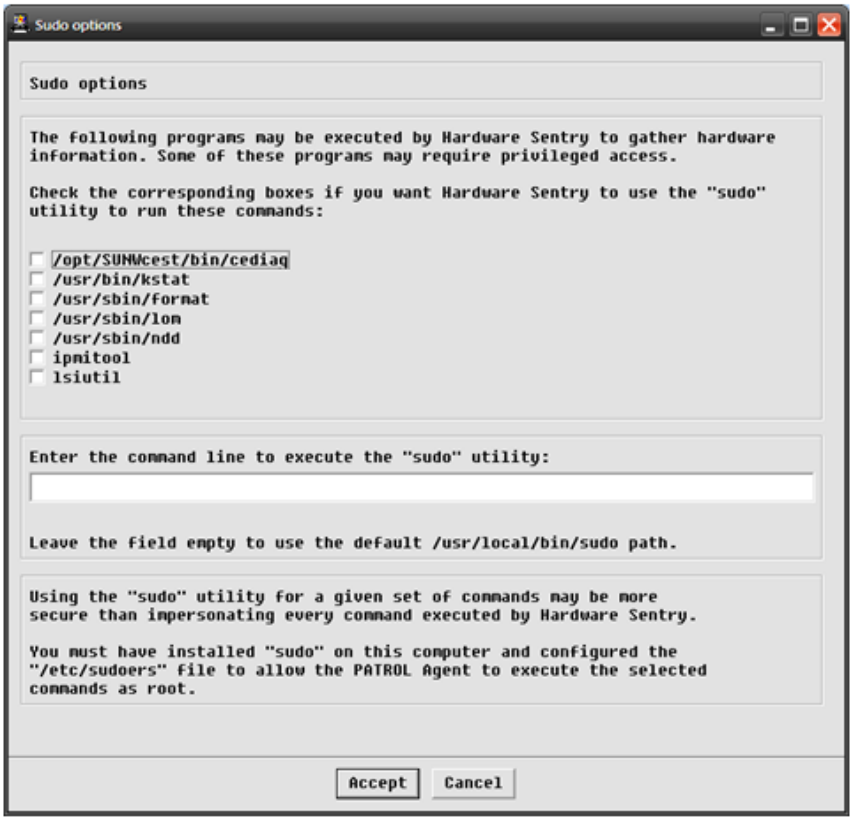
Note

Restart the PATROL agent in order to ensure that the modified settings take effect.

Sudo options (UNIX/Linux)

Depending on the targeted platform, Hardware Sentry may use some external system utilities to gather hardware information. Sometimes the PATROL Agent default account does not have sufficient privileges to execute these commands and it is not possible in your environment to give super-user rights to the PATROL Agent.

In such case Hardware Sentry can use the sudo utility to execute external commands as "root". The sudo utility helps UNIX system administrators secure their environment by authorizing some users to execute only certain commands specified as another user account (typically root). If this applies to you, the sudo options feature could be a good workaround.


Sudo options
Sudo options
The following programs may be executed by Hardware Sentry to gather hardware information. Some of these programs may require privileged access.
Check the corresponding boxes if you want Hardware Sentry to use the "sudo" utility to run these commands:
/opt/SUNWcest/bin/cediag
/usr/bin/kstat
/usr/sbin/format
/usr/sbin/lom
/usr/sbin/ndd
ipmitool
lsiutil
Enter the command line to execute the "sudo" utility:
Leave the field empty to use the default /usr/local/bin/sudo path.
Using the "sudo" utility for a given set of commands may be more secure than impersonating every command executed by Hardware Sentry.
You must have installed "sudo" on this computer and configured the "/etc/sudoers" file to allow the PATROL Agent to execute the selected commands as root.
Accept
Cancel

- **Commands**: Select the commands Hardware Sentry should execute using the sudo utility.
- **Command line to execute the sudo utility**: Enter the command line, or, leave the field blank to use the default /usr/local/bin/sudo path.

Note

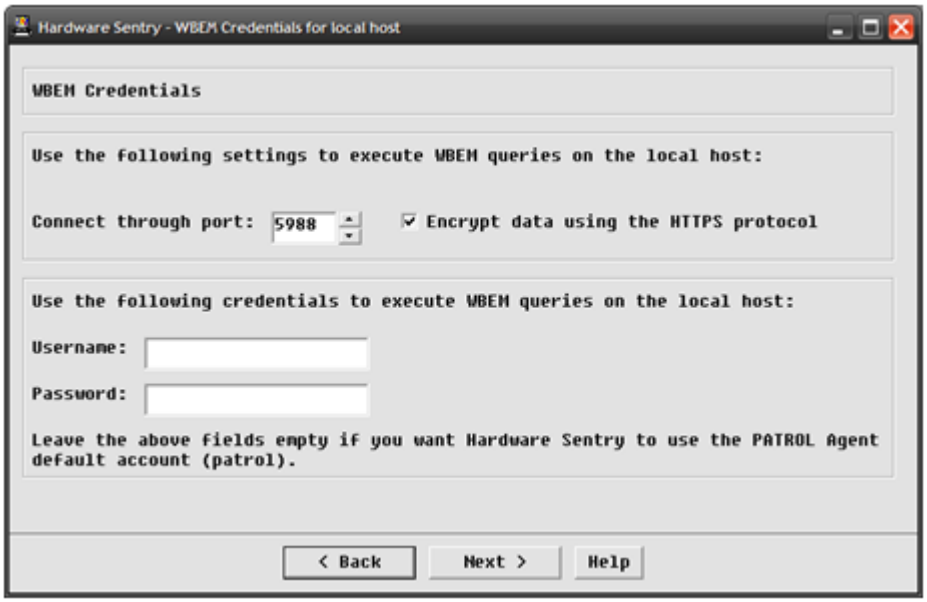
Ensure that the sudo utility is installed on the system, and that the "/etc/sudoers" file is configured to allow the PATROL Agent to execute the selected commands as root.

Here is the procedure to configure Hardware Sentry to use "sudo":

1. Identify the commands run by Hardware Sentry that require advanced privileges.
2. Configure "sudo" to allow the PATROL Agent default account to execute the needed commands as root (modify the /etc/sudoers file). Configuring "sudo" requires root privileges.
3. Check that the PATROL Agent default account is properly authorized to execute the needed commands through the "sudo" utility.
4. Access the Hardware Sentry Security Settings panel: **Hardware icon** > **This Systems's Setting > Connection, Credentials and Connectors > Sudo options**.
5. Check the boxes corresponding to the commands that have been configured in "sudo".

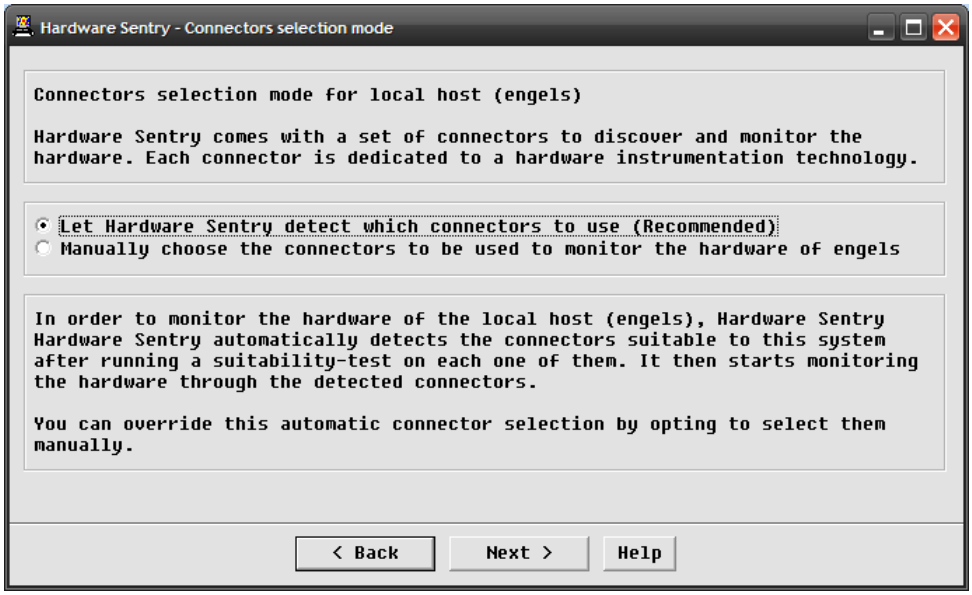
The next panel asks for WBEM credentials:

WBEM credentials


Hardware Sentry - WBEM Credentials for local host
WBEM Credentials
Use the following settings to execute WBEM queries on the local host:
Connect through port: 5988
Encrypt data using the HTTPS protocol
Use the following credentials to execute WBEM queries on the local host:
Username:
Password:
Leave the above fields empty if you want Hardware Sentry to use the PATROL Agent default account (patrol).
< Back
Next >
Help

Enter the **WBEM credentials** or leave blank if using default PATROL account credentials and click **Next**. The next panel allows you to decide which mode is to be used for selecting connectors.

Connector selection


Hardware Sentry - Connectors selection mode
Connectors selection mode for local host (engels)
Hardware Sentry comes with a set of connectors to discover and monitor the hardware. Each connector is dedicated to a hardware instrumentation technology.
Let Hardware Sentry detect which connectors to use (Recommended)
Manually choose the connectors to be used to monitor the hardware of engels
In order to monitor the hardware of the local host (engels), Hardware Sentry Hardware Sentry automatically detects the connectors suitable to this system after running a suitability-test on each one of them. It then starts monitoring the hardware through the detected connectors.
You can override this automatic connector selection by opting to select them manually.
< Back
Next >
Help

Two choices are possible:

- **Let Hardware Sentry detect which connectors to use**: In this mode, Hardware Sentry will run tests at each discovery and select the connectors that best match the managed system.
- **Manually choose the connectors**: Selecting this option lets *you* decide which connectors Hardware Sentry should use to monitor the system Hardware.

Note

When the panel comes up, the selected option is the one that is currently in use.

Automatic selection

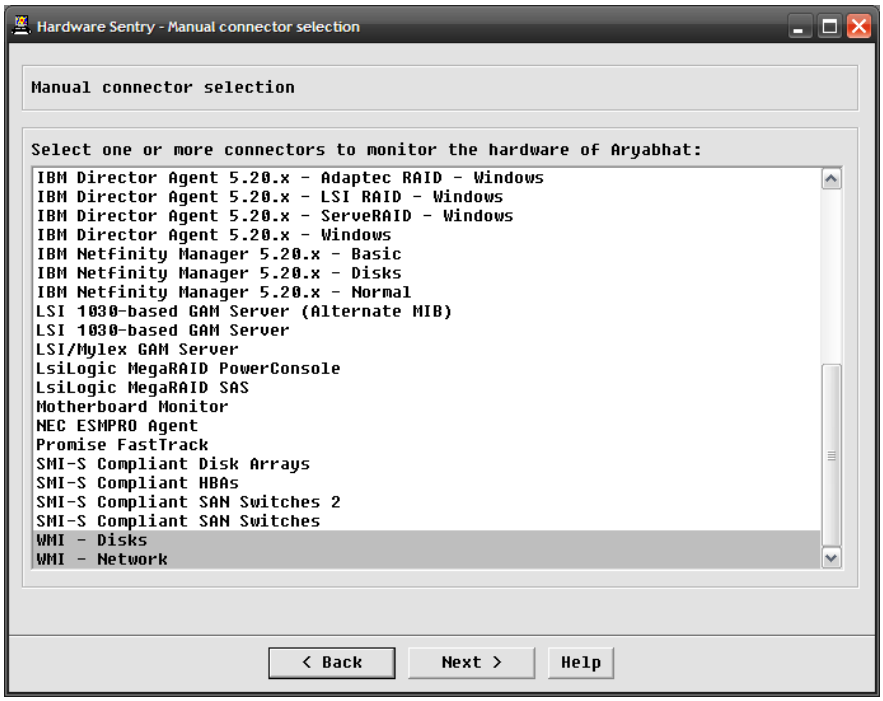
The first option: **Let Hardware Sentry detect which connectors to use** is recommended and is used by default when Hardware Sentry t is loaded on a PATROL Agent.

The detection process is very efficient and accurate, and generally, does not use the computer's resources extensively.

Clicking on the **Next** button will bring up a panel with a message stating that Hardware Sentry needs to be **reinitialized** to run the detection process again.

Manual selection of connectors

If manual selection is chosen (essential for remote monitoring), the next panel displays a list of connectors to choose from:


Hardware Sentry - Manual connector selection
Manual connector selection
Select one or more connectors to monitor the hardware of Aryabhat:
IBM Director Agent 5.20.x - Adaptec RAID - Windows
IBM Director Agent 5.20.x - LSI RAID - Windows
IBM Director Agent 5.20.x - ServeRAID - Windows
IBM Director Agent 5.20.x - Windows
IBM Netfinity Manager 5.20.x - Basic
IBM Netfinity Manager 5.20.x - Disks
IBM Netfinity Manager 5.20.x - Normal
LSI 1030-based GAM Server (Alternate MIB)
LSI 1030-based GAM Server
LSI/Mylex GAM Server
LsiLogic MegaRAID PowerConsole
LsiLogic MegaRAID SAS
Motherboard Monitor
NEC ESMPRO Agent
Promise FastTrack
SMI-S Compliant Disk Arrays
SMI-S Compliant HBAs
SMI-S Compliant SAN Switches 2
SMI-S Compliant SAN Switches
WMI - Disks
WMI - Network
< Back
Next >
Help

It is possible to select several connectors from the list by simply clicking on them. De-selecting a connector is also performed by clicking on the item on the list..

Note

At the end of the selection wizard, Hardware Sentry runs a full discovery. All devices and sensors are re-detected. If the connector list differs from what Hardware Sentry was using previously, new devices monitored may appear in the PATROL Console and old ones may be removed. If this is the case, pay close attention to the PATROL System Output Window for error messages. A poor selection of connectors may remove all devices and sensors and may prevent Hardware Sentry from being able to monitor the system's hardware!

Final step

Clicking on the **Next** button will bring up a panel with a message stating that Hardware Sentry needs to be **reinitialized** to run the detection process again.

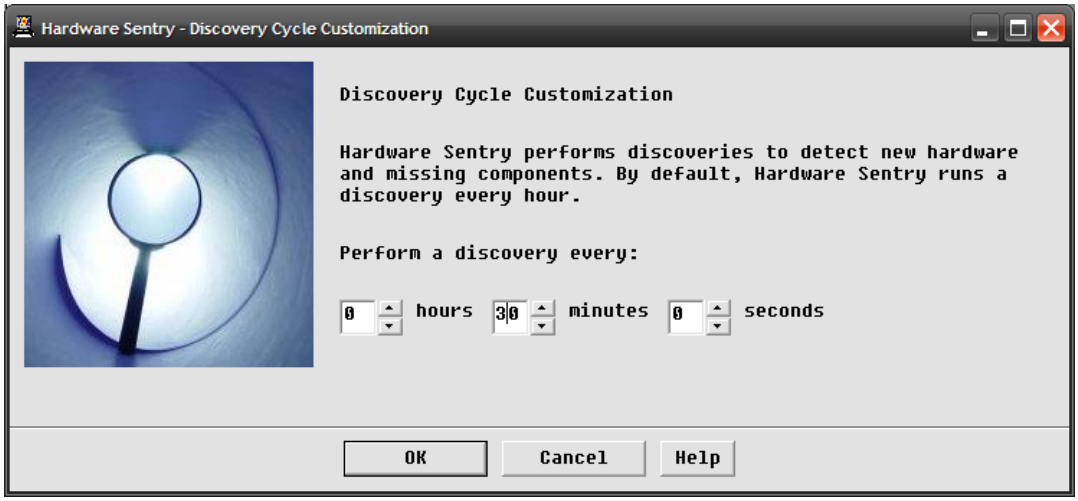
Hardware Sentry - Reinitialize
Reinitialize Hardware Sentry
Hardware Sentry needs to be reinitialized for the new settings to be taken into account. It will destroy all previously discovered objects and trigger a new platform detection on localhost as well as a full discovery of the environment.
Click the Finish button to apply the new settings and reinitialize Hardware Sentry.
< Back
Finish
Help

Click **Finish**.

Customize the discovery cycle

Hardware Sentry performs discoveries to detect new hardware components or detect those that have gone missing.

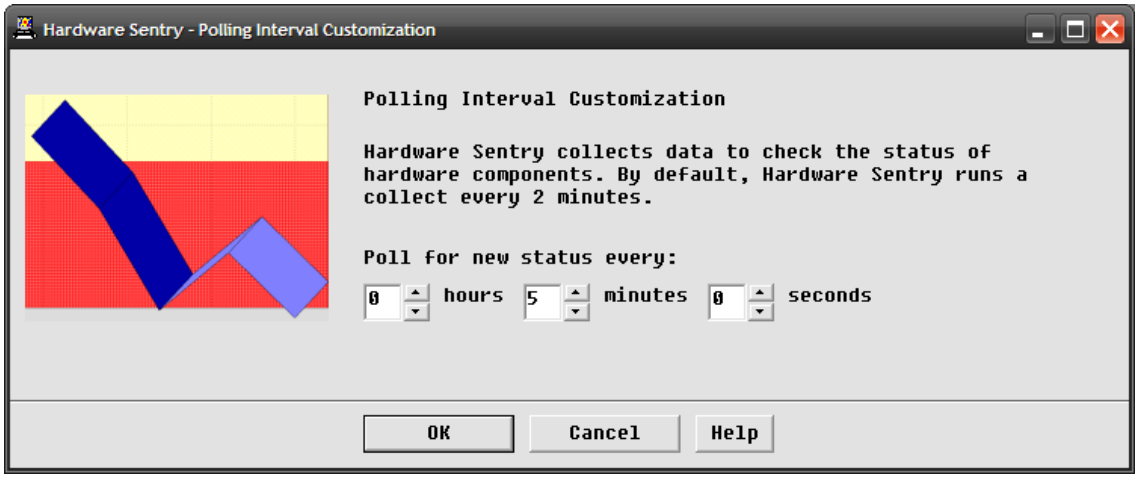
By default, the Hardware Sentry runs a discovery every hour, but you can customize this interval by right-clicking on the **Hardware icon > KM Commands > KM Settings > Discovery Interval.**


Hardware Sentry - Discovery Cycle Customization
Discovery Cycle Customization
Hardware Sentry performs discoveries to detect new hardware and missing components. By default, Hardware Sentry runs a discovery every hour.
Perform a discovery every:
0 hours 30 minutes 0 seconds
OK
Cancel
Help

Customize the polling interval

Hardware Sentry polls the managed systems to collect hardware health data. By default, the polling interval for this "data-collect" is set to every 2 minutes.

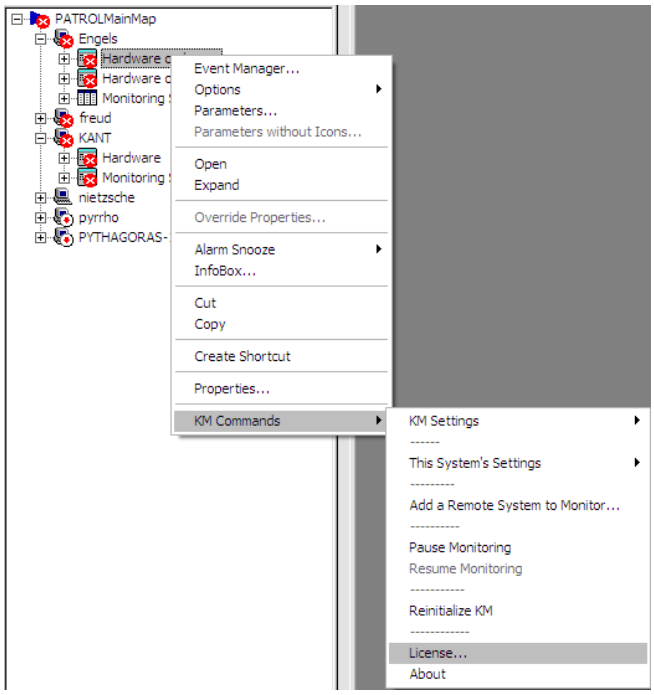
To change the polling interval for the managed system, right-click on **the Hardware icon > KM Commands > KM Settings > Polling Interval:**


Hardware Sentry - Polling Interval Customization
Polling Interval Customization
Hardware Sentry collects data to check the status of hardware components. By default, Hardware Sentry runs a collect every 2 minutes.
Poll for new status every:
0 hours 5 minutes 0 seconds
OK
Cancel
Help

Note

In addition to the polling interval that is a global setting, i.e. it is applicable to the whole managed system; you can also manually trigger a poll at any time on individual instances to refresh parameter values. Right-click on the **instance icon > Refresh Parameters**

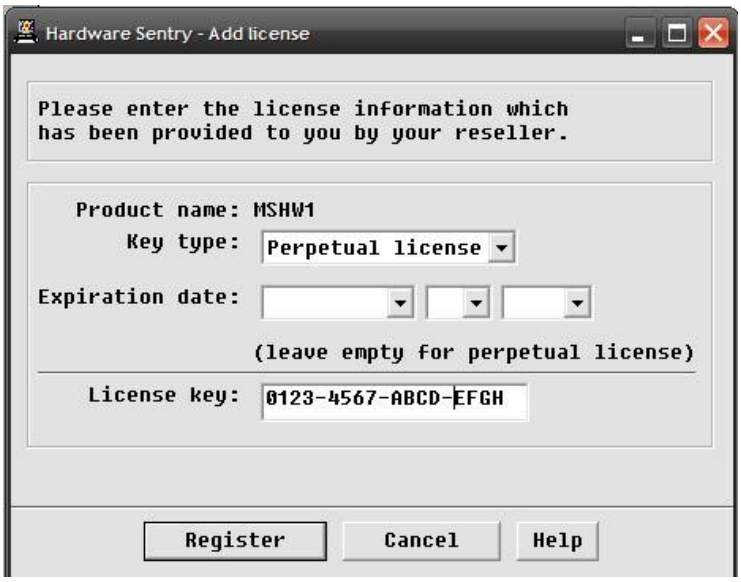
Enter a license key for Hardware Sentry



Right-click on the main **Hardware icon** > **KM Commands > License…**

A dialog box appears and shows the license Hardware Sentry is currently working with (automatic 30-day trial, term license or perpetual license).

To enter a new license key, click on the **Register a new license** button.



Choose the key type depending on the license you purchased (perpetual license or term license).

- For a **Term** License: Enter your Term License expiry date
- For a **Perpetual** License: Leave the expiry- date field blank
- For a **Trial Extension**: Enter the new expiration date

Then, enter your license key in the last field and click on **Register**.

Once the license key has been accepted, the license dialog box is refreshed and shows the new license as registered.

Note

The automatic trial period is always shown in this panel even if it has expired and another license type is valid. This has no effect on the activation of Hardware Sentry.

Distribute the license over several computers

Using a configuration variable

The first way to distribute the Hardware Sentry license key to several computers is to deploy the corresponding configuration variable through wpconfig (Windows), xpconfig (Unix/Linux) or through PATROL Configuration Manager (PCM).

1. On the first computer, enter the license key through the graphical user interface as described in the previous section.

2. Use, **xpconfig, wpconfig** or **PATROL Configuration Manager** to retrieve the **/SENTRY/HARDWARE/license4** configuration variable that has been set by the graphical user interface on the first computer.

3. Distribute this **/SENTRY/HARDWARE/license4** configuration variable to all of the hosts that run Hardware Sentry, through wpconfig, xpconfig or PCM.

The license key distributed through this mechanism will take effect within an hour.

Using a file

The other way to distribute the Hardware Sentry license key to several computers is to deploy the corresponding file through any file distribution mechanism (Distribution Server, Marimba, ftp, etc.)

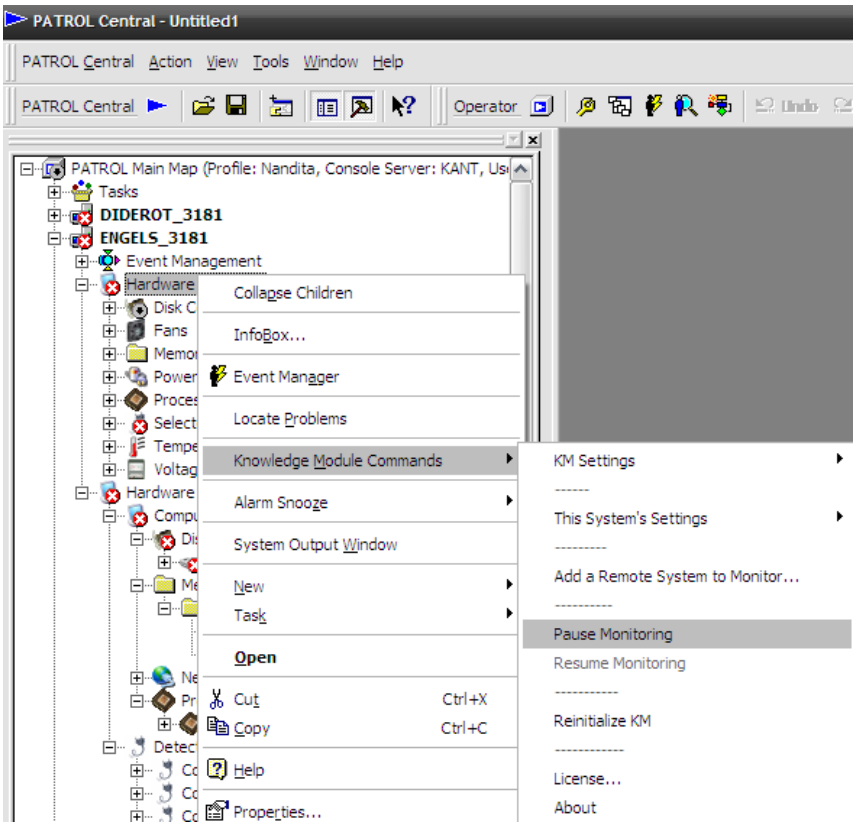
1. On the first computer, enter the license key through the graphical user interface as described in the previous section.

2. Retrieve the file **%PATROL_HOME%\lib\MS_HW_license4** (alternatively **$PATROL_HOME/lib/MS_HW_license4** under UNIX/Linux)

3. Distribute the MS_HW_license4 file to the **%PATROL_HOME%\lib** directory on all of the hosts that run Hardware Sentry.

The license key distributed through this mechanism will take effect within an hour.

Pause the monitoring of an object



In order to perform certain tasks - maintenance for example, it may be interesting to pause the monitoring of an object (or of the managed system as in the image).

Right-click on the **object or system icon > Knowledge Module Commands > Pause Monitoring**

When in paused state, the object/system is still displayed in the PATROL Console but in an **OFFLINE** status and no collect for that particular object is executed.

To restart the monitoring of the object/system click on **Resume Monitoring** in the menu.

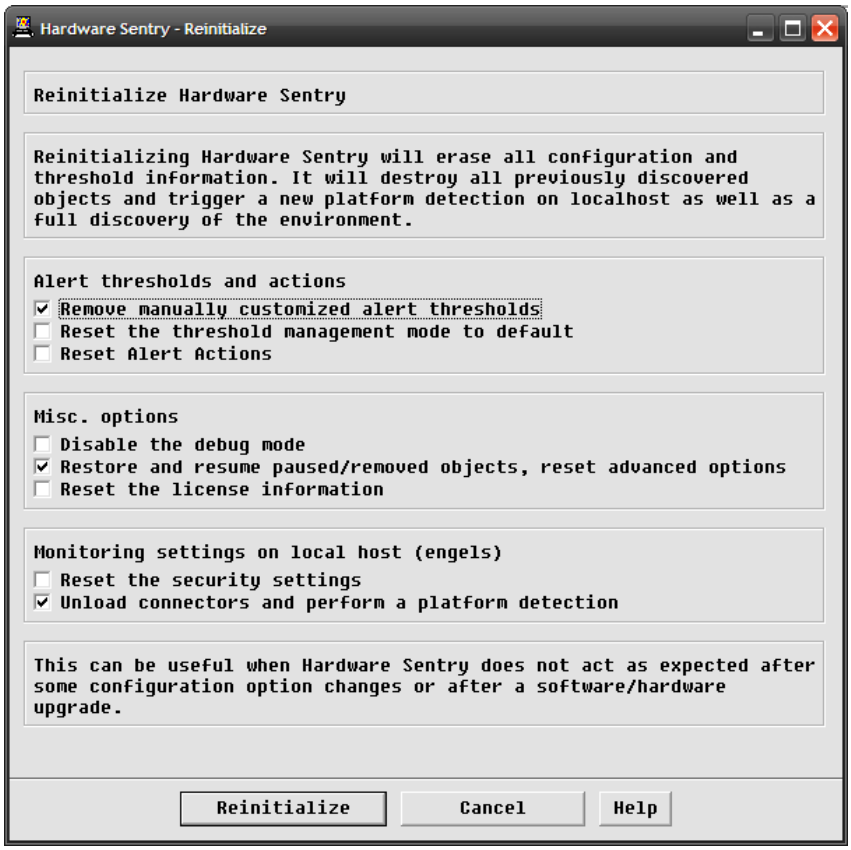
Reinitialize the KM

If ever Hardware Sentry does not function properly: displays devices as missing that you know are present, or does not detect several devices as it should etc., it is possible to reinitialize the configuration and let Hardware Sentry re-start monitoring from scratch.

The above cases of malfunction could occur after a configuration change or especially after a software/hardware upgrade etc.

In such a case, you can reinitialize the KM, and Hardware Sentry will then run a full discovery and will re-detect the managed system, set the appropriate connectors and re-start the monitoring of existing & new devices. Thresholds will be set to default so all previously manually set thresholds will be lost, unless specified otherwise in the **Reinitilize KM** wizard shown below.

To reinitialize Hardware Sentry: Right-click the **Hardware icon > KM Commands > Reinitialize KM**:


Hardware Sentry - Reinitialize
Reinitialize Hardware Sentry
Reinitializing Hardware Sentry will erase all configuration and threshold information. It will destroy all previously discovered objects and trigger a new platform detection on localhost as well as a full discovery of the environment.
Alert thresholds and actions
Remove manually customized alert thresholds
Reset the threshold management mode to default
Reset Alert Actions
Misc. options
Disable the debug mode
Restore and resume paused/removed objects, reset advanced options
Reset the license information
Monitoring settings on local host (engels)
Reset the security settings
Unload connectors and perform a platform detection
This can be useful when Hardware Sentry does not act as expected after some configuration option changes or after a software/hardware upgrade.
Reinitialize
Cancel
Help

Select the options as per your specific needs:

Alert thresholds and actions

- **Remove manually customized alert thresholds**: Selection removes all customized thresholds
- **Reset the threshold mechanism mode to default**: Selection makes the KM revert to the default mode i.e. Hardware Sentry selects the mechanism is best suited to the system.

- **Reset Alert Actions**: Selection removes all manually set Alert Actions and reverts to basic default actions i.e. *Trigger a PATROL event* and *Annotate a parameter graph*.
- **Reset other alert and threshold settings**: Selection reverts any manually done configuration changes to default Hardware Sentry values.

  This is about configuration variables like: pemMessages; disableMissing Device Detection; unexpectedStatusManagement; intrusionDetectionAlert ; parametersMaxOCC or thresholdsFactorization etc.

Note

See the Reference Guide for more details on the Global Configuration Variables and Host-Specific Configuration Variables.

Misc. options

- **Deactivate the debug mode**: Selection deactivates the debug mode if manually enabled.
- **Restore and resume paused/removed object**s: Selection restores all paused or removed objects
- **Remove Hardware Health Report Schedule settings**: Selection clears the report schedule.
- **Reset licensing information**: Selection clears all registered license information.

Monitoring settings for local host only

- **Remove the security settings:** Selection clears all the security settings entered.
- **Unload connectors and perform a platform detection**: Selection restarts the detection process

Click on **Reinitialize**.

Note

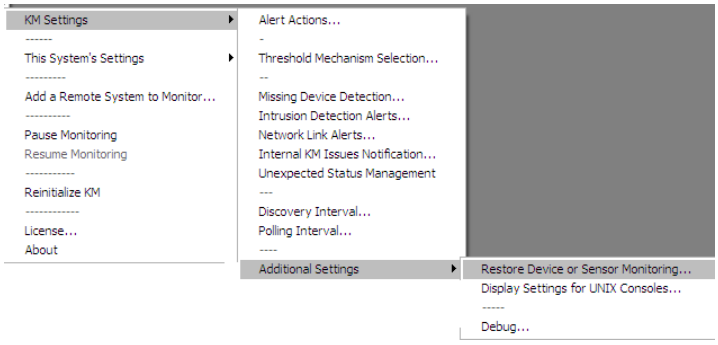
In cases where configurations have been manually set in the PATROL Agent, there will be an additional section called Internal KM engine options displaying the used configuration variables and the option whether or not to remove them.

Note

After reinitializing Hardware Sentry it is not possible to go back to the previous configuration and by default all customizations will be lost (or as per the options selected in the wizard).

Restore the monitoring of a device after removal

It is possible to restore device monitoring with Hardware Sentry after it has been removed from monitoring through the **Remove** option.

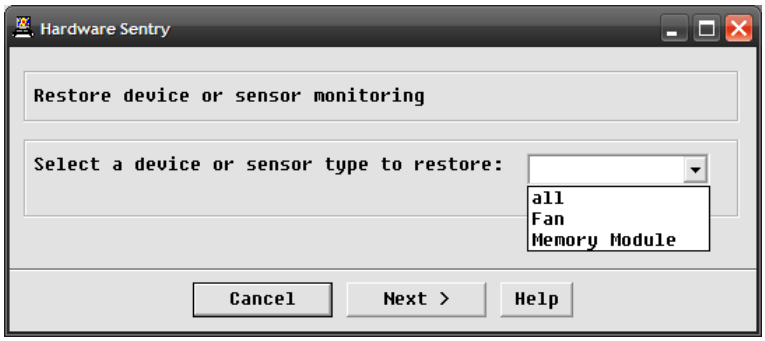


To check the list of the removed objects or to restore a device monitoring:

Right-click the **Hardware icon > KM commands > KM Settings > Additional settings > Restore Device or Sensor Monitoring**

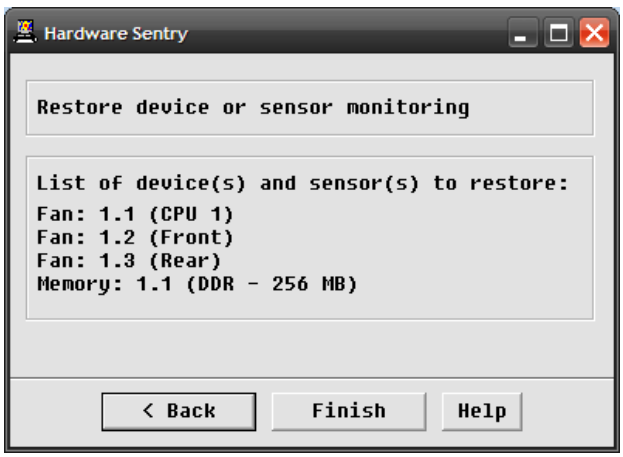
If no object was removed, a message will appear stating that restoration cannot be performed.

Otherwise, the first window of the Restore wizard will pop-up:



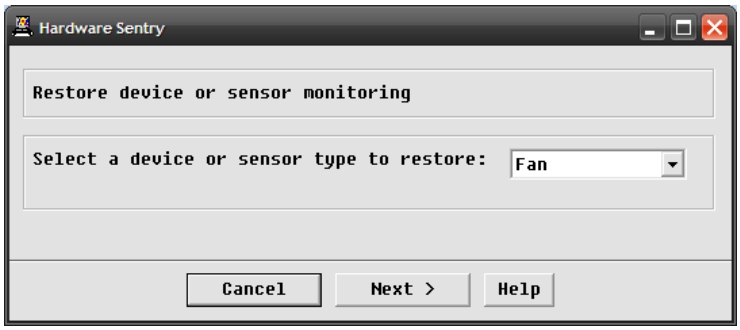
Select the device/s whose monitoring you would like to restore.

For example, here the devices removed were **Fan** and **Memory module**; therefore they appear as options in the list.

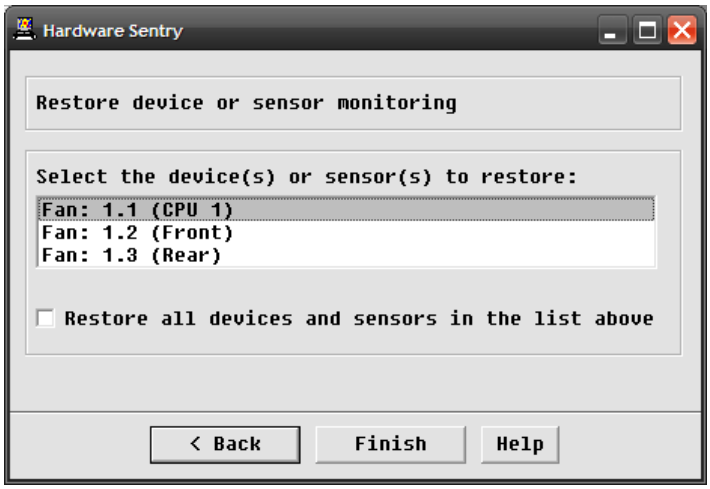


Restore **All** the removed objects, and you see the list of all devices that will be restored.

OR



Select just an individual device and the next panel will show you a list where you can choose between the "sub-devices" of the device as in the case of Fan…



Either select the option **Restore all devices and sensors in the list above**, or select an individual component, and click **Finish**.

Note

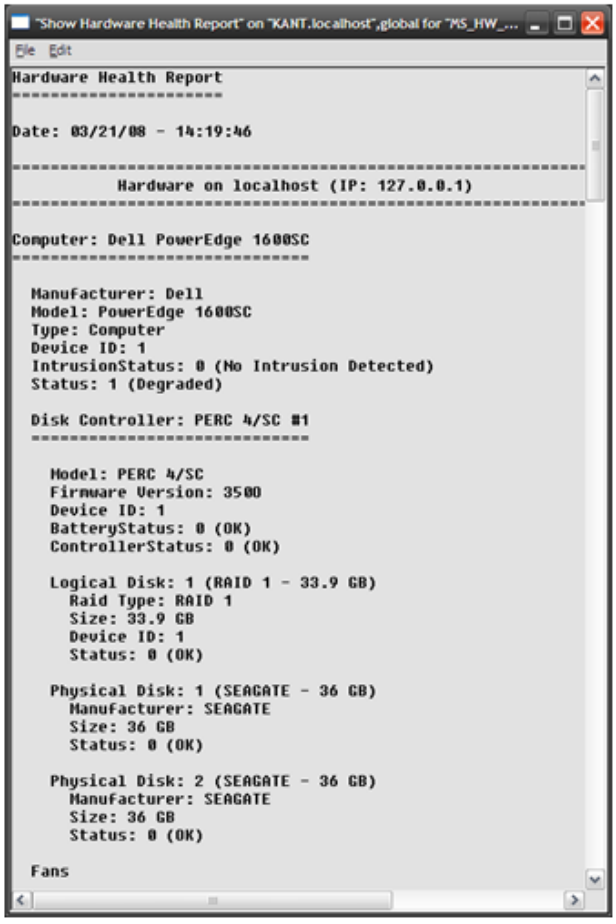
Had you have chosen to restore **All devices and sensors** monitoring in the first window; this second window would just display the list of devices that would be restored.

Show an instant Hardware Health report

The **Instant Hardware Health Report** KM command enables you to generate an instant report on the hardware health of the selected managed system as whole or a report for an individual hardware component.

Report for the entire monitored system/remote device

You can view the hardware health report for the monitored system as a whole i.e. the local host or the remote device by right-clicking on the **Hardware/Hardware on "remote device" icon > KM Commands > Instant Hardware Health Report**.

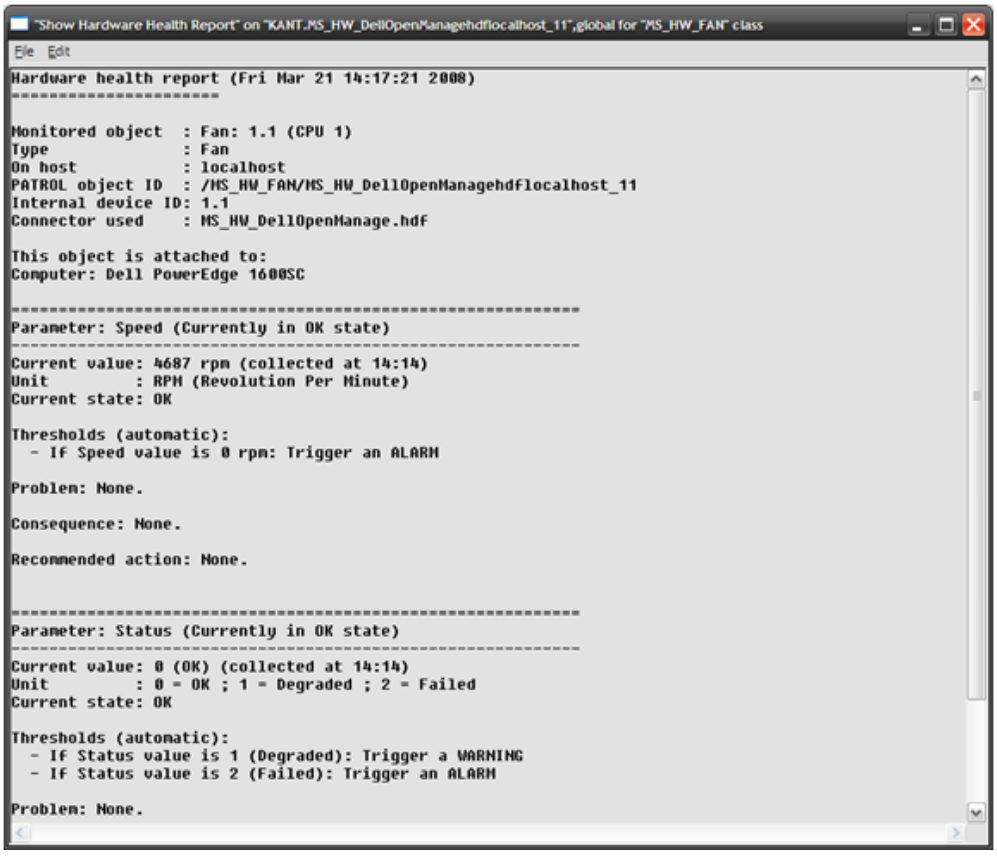


- For a local host, the report will state: **Hardware on <localhost>**
- For a remotely monitored system/device, the report will state: **Hardware on <remote host name>**

This report gives complete information on the hardware health of the managed system. It lists all the hardware components monitored on that system/remote device with details on parameters, thresholds, connectors etc., as well as a description of errors or problems encountered, the possible consequences, and the actions recommended to resolve the issues, if any.

Report for each hardware component

You can view the hardware health report of each monitored hardware component by right-clicking on the **component icon > KM Commands > Instant Hardware Health Report**.


"Show Hardware Health Report" on "KANT.MS_HW_DellOpenManagehdflocalhost_11",global for "MS_HW_FAN" class
File Edit
Hardware health report (Fri Mar 21 14:17:21 2008)
Monitored object : Fan: 1.1 (CPU 1)
Type : Fan
On host : localhost
PATROL object ID : /MS_HW_FAN/MS_HW_DellOpenManagehdflocalhost_11
Internal device ID: 1.1
Connector used : MS_HW_DellOpenManage.hdf
This object is attached to:
Computer: Dell PowerEdge 1600SC
Parameter: Speed (Currently in OK state)
Current value: 4687 rpm (collected at 14:14)
Unit : RPM (Revolution Per Minute)
Current state: OK
Thresholds (automatic):
- If Speed value is 0 rpm: Trigger an ALARM
Problem: None.
Consequence: None.
Recommended action: None.
Parameter: Status (Currently in OK state)
Current value: 0 (OK) (collected at 14:14)
Unit : 0 = OK ; 1 = Degraded ; 2 = Failed
Current state: OK
Thresholds (automatic):
- If Status value is 1 (Degraded): Trigger a WARNING
- If Status value is 2 (Failed): Trigger an ALARM
Problem: None.

This health report gives information about the monitored object (parameters, thresholds, connectors etc.) as well as a description of the problems encountered, the possible consequences, and recommended actions.

Note

To schedule a regular hardware health report on an hourly, daily, weekly or monthly basis for a managed system, please see the related topic: *Schedule Hardware Health reports*

Schedule Hardware Health reports

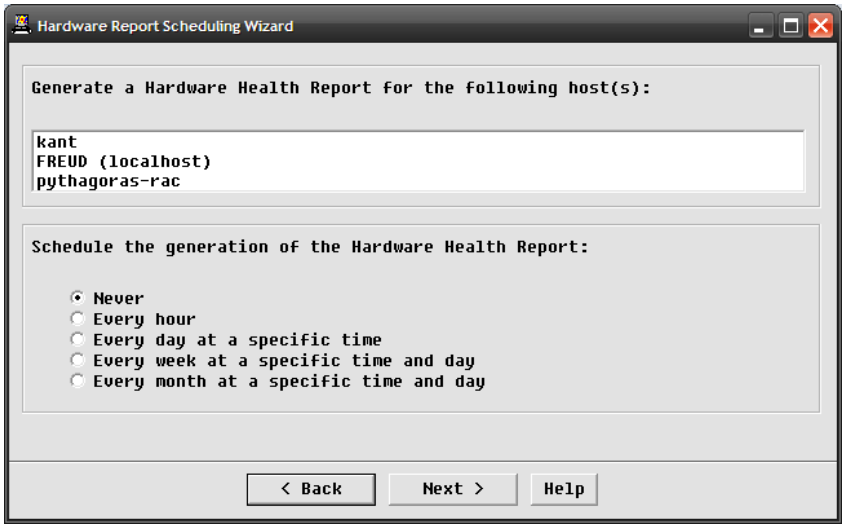
Hardware Sentry enables you to schedule automated generation of hardware health reports for the locally managed systems as well as the remotely monitored hosts/devices.

To schedule a hardware health report, right-click on **the Hardware icon > KM Commands > Schedule Hardware Health Reports**

1. The Hardware Health Scheduling wizard appears

Hardware Report Scheduling Wizard
Welcome to the Hardware Report Scheduling wizard.
This wizard allows you to schedule a report of the current status of the hardware components monitored on FREUD
Watching over your IT infrastructure
Cancel
Next >
Help

2. The next panel asks you to select the hosts and schedule the report:


Hardware Report Scheduling Wizard
Generate a Hardware Health Report for the following host(s):
kant
FREUD (localhost)
pythagoras-rac
Schedule the generation of the Hardware Health Report:
Never
Every hour
Every day at a specific time
Every week at a specific time and day
Every month at a specific time and day
< Back
Next >
Help

The host selection fields display the locally managed system as well as all remote devices/systems monitored remotely on the local host.

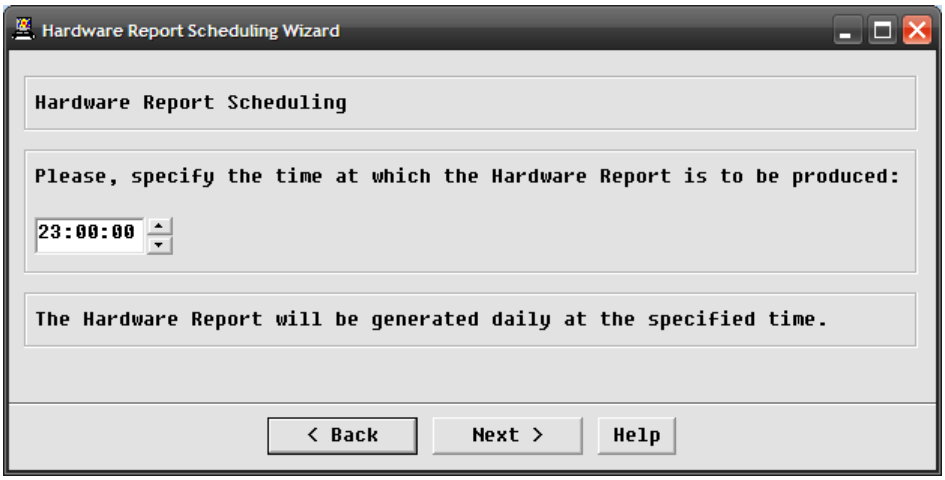
- **Generate a Hardware Health Report for the following hosts**: Select the hosts

- **Schedule the report: Never/Every hour/Every day at a specific time/ Every week at a specific time and day/Every month at a specific time and day**

Click **Next**.

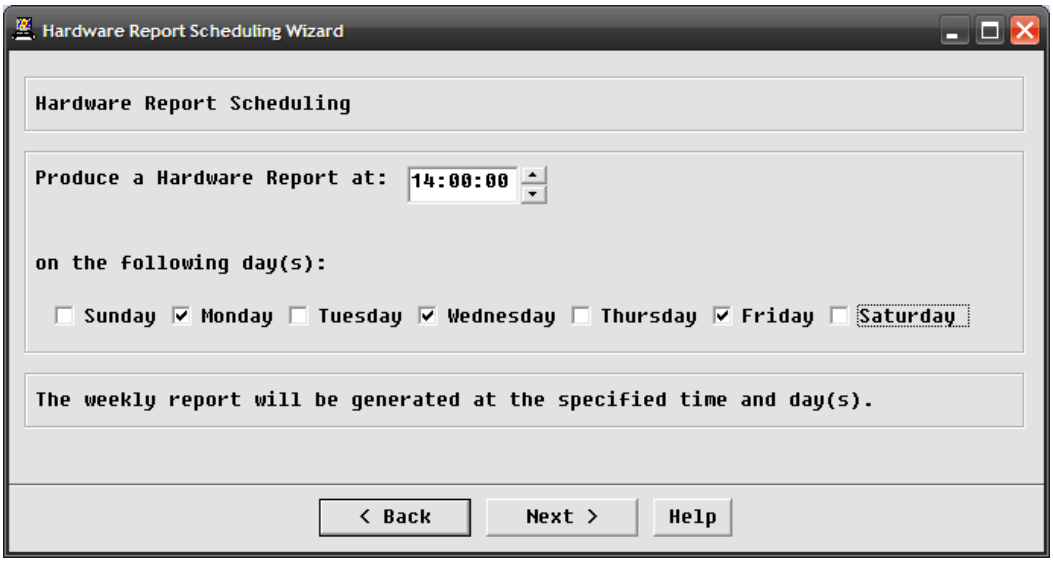
3. Depending on the schedule selected, the following panels will appear:

Every day at a specific time:


Hardware Report Scheduling Wizard
Hardware Report Scheduling
Please, specify the time at which the Hardware Report is to be produced:
23:00:00
The Hardware Report will be generated daily at the specified time.
< Back
Next >
Help

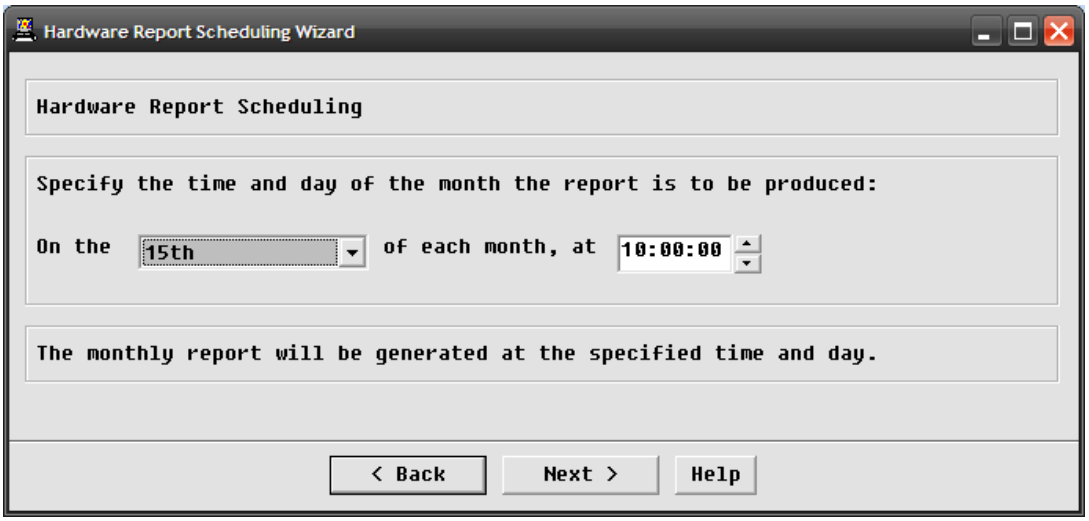
Indicate the time at which the report is to be generated and click **Next**.

Every week at a specific time and day:



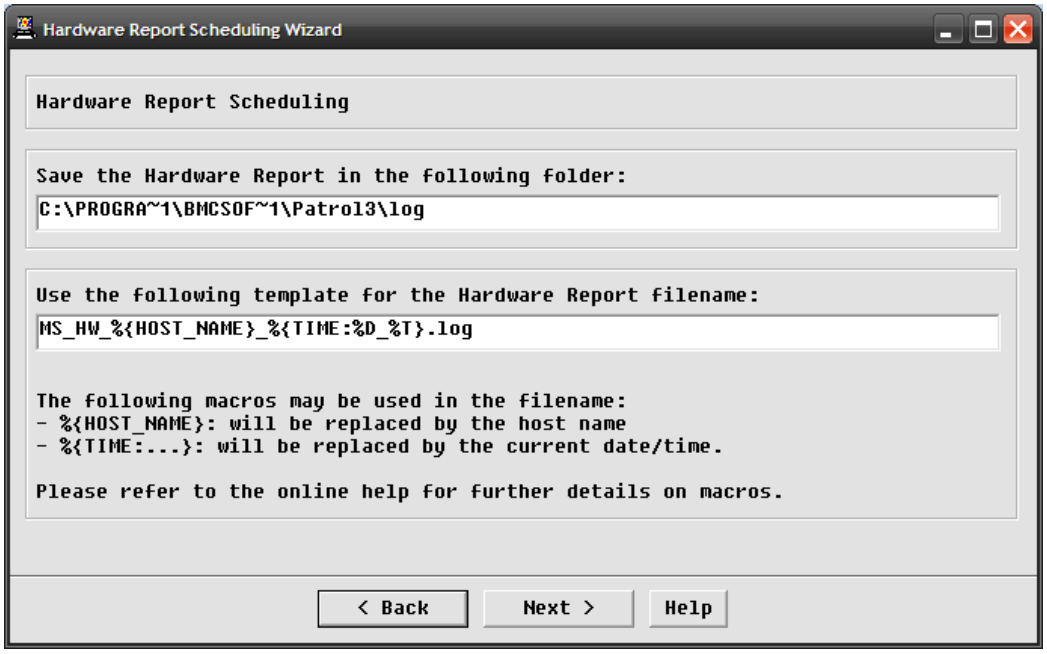
Specify the time and the days you want the report generated and click **Next**.

Every month at a specific time and day:


Hardware Report Scheduling Wizard
Hardware Report Scheduling
Specify the time and day of the month the report is to be produced:
On the 15th of each month, at 10:00:00
The monthly report will be generated at the specified time and day.
< Back
Next >
Help

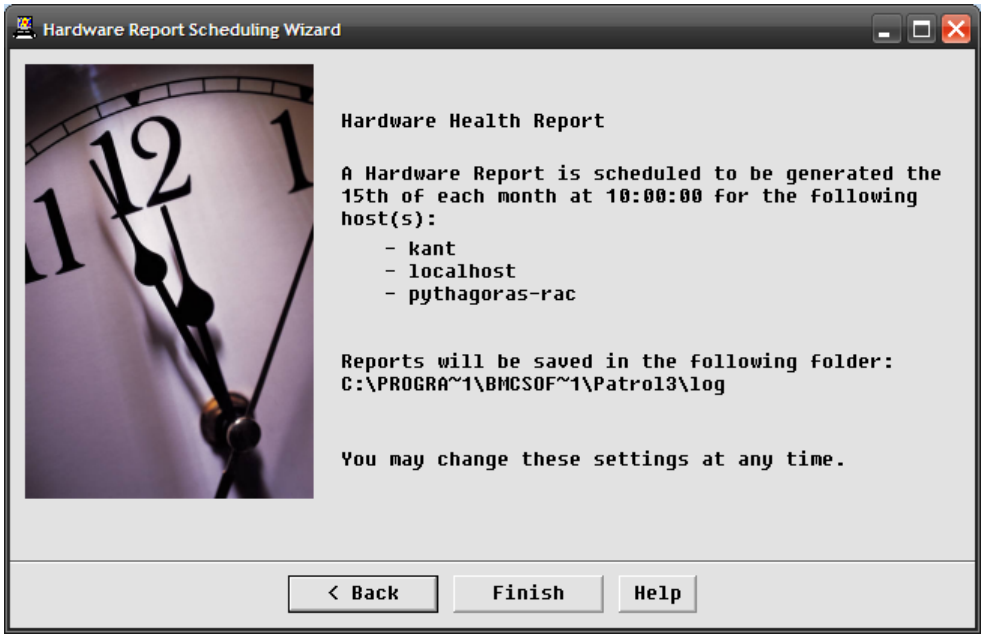
Indicate the day of each month and the time at which the report is to be generated and click **Next**.

4. Indicate where the report is to be saved and specify its filename:


Hardware Report Scheduling Wizard
Hardware Report Scheduling
Save the Hardware Report in the following folder:
C:\PROGRA~1\BMCSOF~1\Patrol3\log
Use the following template for the Hardware Report filename:
MS_HW_%{HOST_NAME}_%{TIME:%D_%T}.log
The following macros may be used in the filename:
- %{HOST_NAME}: will be replaced by the host name
- %{TIME:...}: will be replaced by the current date/time.
Please refer to the online help for further details on macros.
< Back
Next >
Help

- **Save the Hardware Health Report in the following folder**: Enter the file path
- **Use the following template for the Hardware Health Report filename**: Using the given macros will enable you to have reports that are properly named with the hostname and time the reports are generated. You can refer to the *Macros* in the Reference guide or in the online help for more details.

5. Hardware Health Report confirmation:

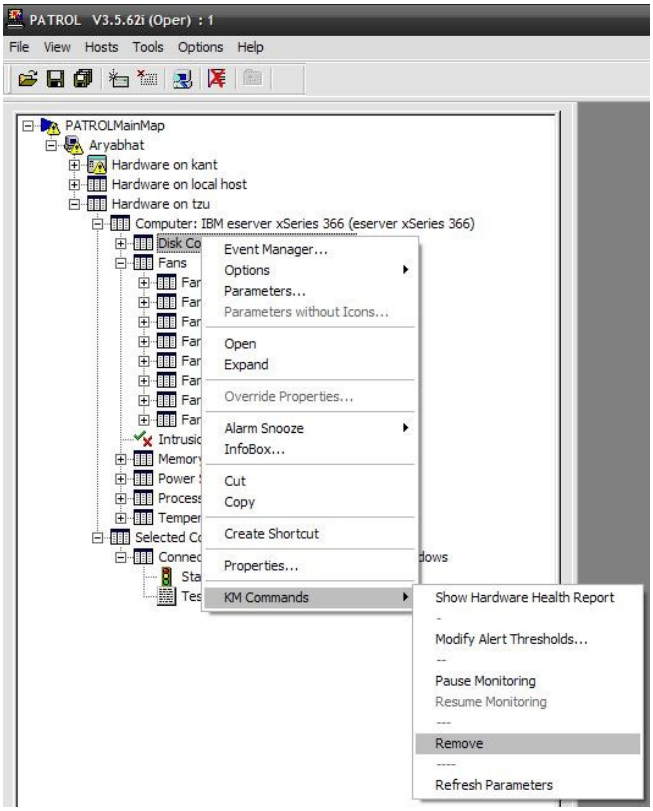

Hardware Report Scheduling Wizard
Hardware Health Report
A Hardware Report is scheduled to be generated the 15th of each month at 10:00:00 for the following host(s):
- kant
- localhost
- pythagoras-rac
Reports will be saved in the following folder:
C:\PROGRA~1\BMCSOF~1\Patrol3\log
You may change these settings at any time.
< Back
Finish
Help

Click **Finish**. You can change these settings at any time.

You can also generate an Instant Hardware Health report at any time for the whole managed system or for any individual component. See *Show an instant Hardware Health report*

Terminate the monitoring of a device

Information about a device may be received by Hardware Sentry through two different sources. In such a (rare) case, the monitoring of the device is performed twice and the device icon will also appear twice in the PATROL Console.



In order to avoid such redundancy, the solution is a simple: remove one of the devices monitored in the PATROL Console:

Right-click the **sensor/device** you wish to remove **> KM Commands > Remove**.

The device is now removed from monitoring which means collection for this particular device will no longer be performed, and the redundant icon representing the device will disappear from the PATROL Console.

Trigger a KM discovery

Hardware Sentry automatically executes a discovery every hour of all hardware objects for the monitored system. This enables discovering and then monitoring any new objects added or removed etc.

You can also **force a discovery manually** by right-clicking on the **Hardware icon > KM Commands > Trigger a KM Discovery**

Note

With a view to optimization, the discovery process is as parallelized as possible. All independent objects are processed at the same time.

Display labels in the UNIX Console mode

The PATROL UNIX Console has a label size limitation. This could mean that the at times, object lables do not display in their entirety.

You can opt to turn on the UNIX Console Mode that modifies all labels to fit the PATROL UNOX Console size limitation: right-click on the **Hardware icon > KM Commands > KM Settings > Additional Settings > Display Settings for UNIX Console**

Warning!

Turning on the UNIX Console mode will affect the labels of ALL PATROL consoles including the Windows Consoles. If you have a mix of UNIX and Windows, it is recommended to leave this feature disabled.

Troubleshooting

This section lists the most frequently asked questions:

- *Enabling the debug mode*
- *Hardware Sentry shows nothing*
- *Shows/Monitors Network Interfaces, but no other components*
- *Servers running Windows or Linux*
- *Special note about SNMP on Windows Server 2003, 2008*
- *Unable to see Disk Controller*

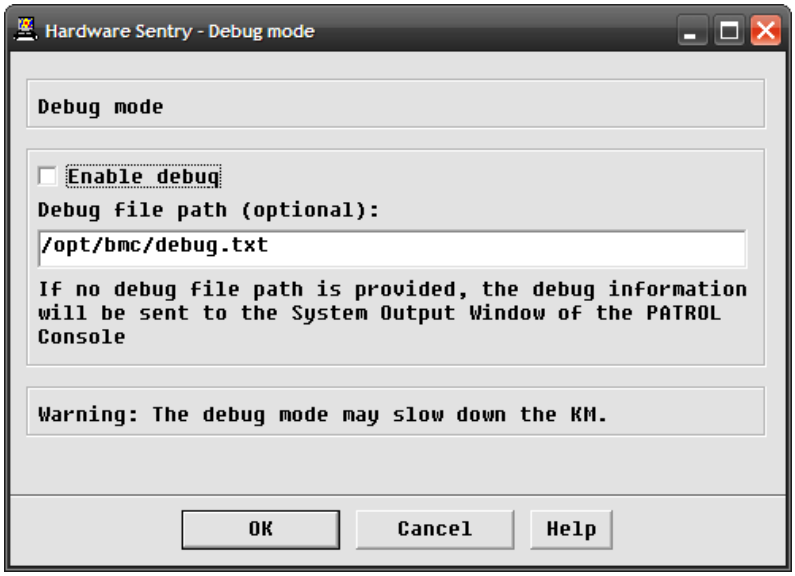
Enabling the debug mode

By default, Hardware Sentry sends only the most critical information, warning and error messages to the System Output Window of the PATROL Consoles. Most often, this information is accurate enough to ensure that Hardware Sentry is working properly.

If you encounter an issue and wish to report it to Sentry Software, you will be asked to enable the Debug Mode and provide the debug output to the Sentry Software support team.

To enable the debug mode:

1. Right-click the main **Hardware icon, KM Commands > This System's Settings > Additional Settings > Debug...**


Hardware Sentry - Debug mode
Debug mode
Enable debug
Debug file path (optional):
/opt/bmc/debug.txt
If no debug file path is provided, the debug information will be sent to the System Output Window of the PATROL Console
Warning: The debug mode may slow down the KM.
OK
Cancel
Help

2. Select **Enable Debug** case and click **OK**.

There could be some loss of debug information by the PATROL console, if debug is enabled just as the PATROL Agent is starting as it is not yet connected to the PATROL Agent. In other cases, or when you want to trace the activity of Hardware Sentry during a few minutes, some debug information may be lost by the PATROL Console owing to a full buffer.

In such cases, it may help to send the debug output of Hardware Sentry to a specified file.

Note

The debug file is stored on the computer where the Agent is running

Warning!

Pay attention to the file size - the debug output of Hardware Sentry could be very large when running for several days.

Hardware Sentry shows nothing

Even if Hardware Sentry is unable to detect any available hardware information source, it should create an icon labeled "Hardware" under the main computer PATROL icon.

If no Hardware Sentry related information is shown at all in the PATROL Console, it means that Hardware Sentry is not running on the Agent, or that an internal error occurred.

Execute the **%DUMP KM_LIST** command in the System Output Window of the PATROL Console. An absence of **MS_HW_MAIN** entry indicates that Hardware Sentry is not loaded on the agent.

1. Ensure sure that the **MS_HARDWARE_SENTRY1.kml** file is preloaded by the PATROL Agent and loaded by the PATROL Consoles, and that the “MS_HW_*.km” are not disabled.

2. See the BMC Software documentation (PATROL Agent Reference Manual) to find out how to load a KM on the PATROL Agent.

3. If the **MS_HW_*** classes are properly loaded and no icon appears in the PATROL Console, it probably means that the Hardware Sentry has not been properly installed on the PATROL Agent.

4. Re-install the KM and ensure that all files are properly installed (typically “*.lib” files in the “`%PATROL_HOME%\lib\psl folder`”)

Shows/Monitors Network Interfaces, but no other components

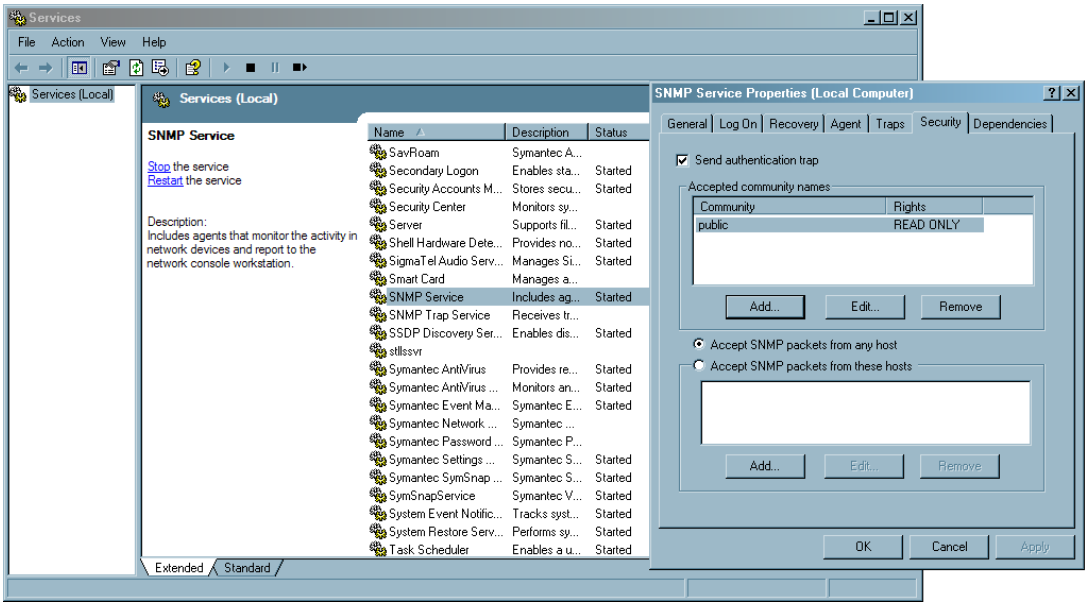
This is typically an SNMP issue. Many manufacturer-provided hardware agents use the SNMP technology (DELL OpenManage, HP Insight Management, Fujitsu-Siemens ServerView and for example). Since Hardware Sentry gathers hardware information from these agents, you need to enable and properly configure the SNMP layer on the managed servers if an SNMP-based agent is running on them.

However sometimes, like in the case of HP® (Compaq®) ProLiant® servers, the network interface is detected and therefore displays in the PATROL Console /Central view whilst no other hardware component gets detected by Hardware Sentry – simply because it cannot communicate with the managed element. So enabling and authorizing the managed server to communicate through the SNMP protocol is essential.

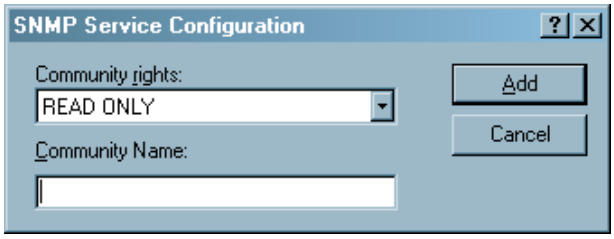
Configuring SNMP on Windows servers 2003

Starting with Windows Server 2003, the SNMP service is not configured to allow the "public" community by default. As a consequence, even if the SNMP service is properly installed and the hardware agent properly running, Hardware Sentry is not able to gather any hardware information from the SNMP agent. Therefore, on Windows Server computers that run an SNMP-based hardware agent (DELL OpenManage, HP Insight Management or Fujitsu-Siemens ServerView), you first need to install the SNMP service (not installed by default) and then configure it to allow a community to access the SNMP agent.

1. In the Services administrative tool, right-click on **SNMP service > Properties**. Click on **Security**:



2. Click on the first **Add** button and enter a community name that will allow access to the SNMP agent (READ ONLY):



3. Click **OK**. The new settings are taken into account immediately. Hardware Sentry will automatically detect the community string that you entered in the security settings of the SNMP service. Note on unsupported servers running Windows or Linux

On officially non-supported servers running Windows or Linux, Hardware Sentry will still be able to monitor network cards and internal, non-RAID disks

Servers running Windows or Linux

Even on officially un-supported servers running Windows or Linux, Hardware Sentry will be able to monitor network cards and internal, non-RAID disks.

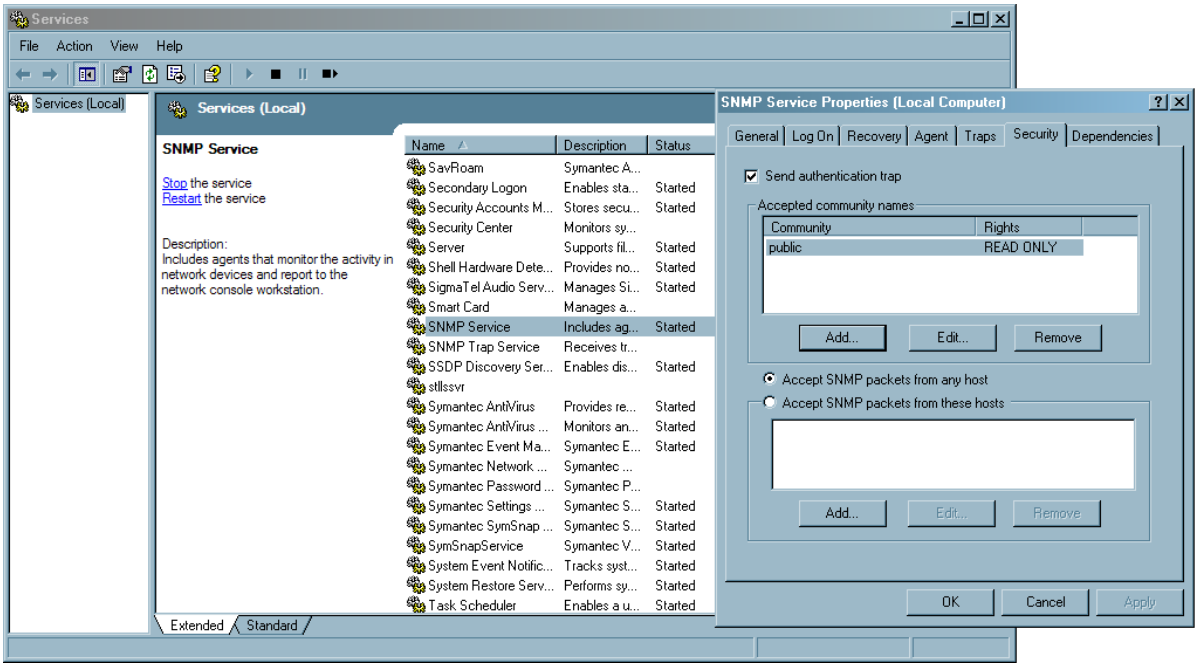
Special note about SNMP on Windows Server 2003, 2008

Many manufacturer-provided hardware agents use the SNMP technology (DELL OpenManage, HP Insight Management, Fujitsu-Siemens ServerView and for example).

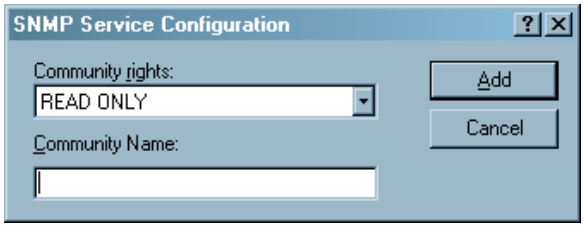
Starting with Windows Server 2003, the SNMP service is not configured to allow the "public" community by default. As a consequence, even if the SNMP service is properly installed and the hardware agent properly running, Hardware Sentry is not able to gather any hardware information from the SNMP agent.

Therefore, on Windows Server 2003 computers that run an SNMP-based hardware agent (DELL OpenManage, HP Insight Management or Fujitsu-Siemens ServerView), you first need to install the SNMP service (not installed by default) and then configure it to allow a community to access the SNMP agent.

1. In the Services administrative tool, right-click on **SNMP service > Properties**. Click on **Security**



2. Click on the **Add** button and enter a community name that will be allowed to access the **SNMP agent (READ ONLY)**:



3. Click **OK**. The new settings are taken into account immediately. Hardware Sentry will automatically detect the community string that you entered in the security settings of the SNMP service.

Unable to see Disk Controller

On some computers, the manufacturer-specific hardware monitoring agent is only responsible for the monitoring of the baseboard: temperatures, fans, voltages and power supplies. In this case, the disk monitoring is handled by the disk controller manufacturer. Therefore, you need to install additional software for your disk monitoring.

Please contact your server vendor to know which software must be used with your disk controller.

Important

See the Connectors & Platforms Reference Table in the Reference Guide and verify if your system has all the required tools/agents installed on it. Also check the details for you system by clicking on the connector name. This will display the objects discovered by Hardware Sentry if all pre-requisites are fulfilled.

Notes

About BMC® Software

BMC Software, Inc. [NYSE:BMC], is a leading provider of enterprise management solutions that empower companies to manage their IT infrastructure from a business perspective. Delivering Business Service Management, BMC Software solutions span enterprise systems, applications, databases, and service management. Founded in 1980, BMC Software has offices worldwide and fiscal 2004 revenues of more than $1.4 billion. For more information about BMC Software, visit www.bmc.com.

About Sentry Software™

Sentry Software, a strategic Technology Alliance Partner of BMC Software, provides key monitoring solutions specifically designed to expand the capabilities of BMC Performance Manager, thus enabling up to 100% coverage of any infrastructure. Sentry Software specializes in single solutions for multi-platform monitoring of hardware, custom applications or any IT component, and blackout windows. Sentry Software products are deployed in 45 countries across the globe and lead the list of BMC Software's third-party product sales. For more information about Sentry Software, please visit www.sentrysoftware.net.